An algebraic approach to graph codes

Pinero, Fernando

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

An algebraic approach to graph codes

Fernando Luis Piñero González

Kongens Lyngby 2014
Compute-PhD-2014-352

Technical University of Denmark
Department of Applied Mathematics and Computer Science
Building 324, DK-2800 Kongens Lyngby, Denmark
Phone +45 45253031, Fax +45 45881199
compute@compute.dtu.dk
www.compute.dtu.dk Compute-PhD-2014-352

Summary (English)

This thesis consists of six chapters. The first chapter, contains a short introduction to coding theory in which we explain the coding theory concepts we use. In the second chapter, we present the required theory for evaluation codes and also give an example of some fundamental codes in coding theory as evaluation codes. Chapter three consists of the introduction to graph based codes, such as Tanner codes and graph codes. In Chapter four, we compute the dimension of some graph based codes with a result combining graph based codes and subfield subcodes. Moreover, some codes in chapter four are optimal or best known for their parameters. In chapter five we study some graph codes with Reed–Solomon component codes. The underlying graph is well known and widely used for its good characteristics. This helps us to compute the dimension of the graph codes. We also introduce a combinatorial concept related to the iterative encoding of graph codes with MDS component code. The last chapter deals with affine Grassmann codes and Grassmann codes. We begin with some previously known codes and prove that they are also Tanner codes of the incidence graph of the point–line partial geometry of the Grassmannian. We expect that the techniques exposed in chapter six are also applicable to other codes as well.

Summary (Danish)

Afhandlingen består af seks kapitler. Kapitel 1 indeholder en kort introduktion til kodningsteori, hvor de begreber og resultater fra kodningsteori der er benyttet i det følgende, bliver gennemgået. I kapitel 2 bliver den relevante teori for evalueringskoder introduceret og en række af de klassiske koder bliver præsenteret som evalueringskoder. Kapitel 3 indeholder konstruktion af koder baseret på grafer, blandt andet Tanner koder og graf koder. I kapitel 4 bestemmes dimensionen af nogle graf baserede koder ved at kombinere resultater om graf koder og subfield subcodes. En del af disse koder er optimale for de givne parametre eller blandt de bedst kendte. I kapitel 5 studerer vi en klasse af graf koder med Reed-Solomon komponentkoder. De underliggende grafer er velkendte og er ofte udnyttede på grund af deres fine kombinatoriske egenskaber. Ved hjælp heraf bestemmes dimensionen af en række grafkoder. Kapitlet indeholder også en introduktion til et kombinatorisk begreb der kan udnyttes til iterativ indkodning af grafkoder med MDS komponentkoder. Det afsluttende kapitel behandler affine Grassmann koder og Grassmann koder. Det vises blandt andet at en bestemt klasse af koder kan opfattes som Tanner koder baseret på incidens grafen af punkter og linier i den såkaldte Grassmann mangfoldighed. Det forekommer sandsynligt at de i kapitel 6 udviklede teknikker ogsåkan anvendes på andre klasser af fejlrettende koder.

Preface

This thesis was prepared at the Department of Applied Mathematics and Computer Science at the Technical University of Denmark in fulfilment of the requirements for acquiring a Ph.D. in mathematics. It collects the work we've done in the last three years on graph based codes. We have focused on an algebraic approach to graph codes. The reason everything works well here is that the algebraic aspect of the graphs we study complements nicely the algebraic structure of the component codes. Therefore, we can set both the codes and the graphs under the same algebraic framework. After this, we obtained some good results on the dimension of graph codes including the optimality and near optimality of the dimension is some cases with Reed–Solomon component codes and the characterization of the dual code of a graph code.

We also obtained some results about Grassmann codes and affine Grassmann codes. We were able to characterize the minimum weight codewords of the dual Grassmann codes and dual Affine Grassmann codes. In turn, this implies that Grassmann codes are Tanner codes where the graph is the point–line incidence graph of the point–line partial geometry of the Grassmannian. The partial geometry of the Grassmannian captures the algebraic and geometrical essence of the Grassmannian, and this is also reflected on the Grassmann code. Furthermore, we also proved that the Grassmann code has optimal dimension with respect to the graph and MDS component code. We were able to extend this to an iterative encoding function of the Grassmann code as a Tanner code.

The difference between the techniques used for both classes of codes is that, for the codes in Chapter four and five, we began with a graph and a component code and we combined the two together to make graph codes, which we study. Using the inherent algebraic structure of the graph and the component codes we

were able to put the whole graph code on the same algebraic framework. This allowed us to bound their dimension.

For the codes in Chapter six we began with a known code: the Grassmann code. From the algebraic properties of the Grassmannian we knew the Grassmann codes are contained in a nontrivial Tanner code. We were able to use the characterization of a Tanner code in terms of projections and the minimum weight codewords of the Grassmannian to prove that actually the Grassmann codes are the Tanner codes of the point–line geometry of the Grassmannian. In this case, we used the Tanner code concept to study a well known code.

We feel both codes represent an exchange between coding theory and algebraic geometry. The codes in Chapter four and five have graphs which represent a finite projective geometry. Furthermore, the component codes also represent geometrical objects inherent to the geometry of the Grassmannian. Commutative algebra blends the two together in a way which preserves the graph code construction. This represents an application of Algebraic Geometry to Coding Theory. The codes in Chapter six are essentially an algebraic geometrical object. From the algebraic geometrical properties of the codes we can prove they are Tanner codes in a nontrivial way. Moreover, this Tanner code also reflects the algebraic geometrical properties of the original code. In this way Coding Theory is applied to Algebraic Geometry.

Both approaches are useful in coding theory. Both approaches were quite pleasing to work with. The work on these classes of codes is not yet exhausted. We hope to use the results in this Ph.D. thesis to expand results in coding theory.

Lyngby, 31 October-2014

Fernando Luis Piñero González

Acknowledgements

I would like to take this opportunity to thank the following:

- *To Mom*: Your love and support is felt halfway around the world.
- *To Dad*: I always follow your example to Victory!
- *To Rebecca*: The adventures in life without you would not have been the same. Thank you for at least 12 great years.
- *To Siggy*: The adventures with you are now completely different than what they were before you.
- *To Peter*: Thank you for your professionalism. It is something to aspire to.
- *To Tom*: You and your hard work made this possible. It is something I will always appreciate and never forget.
- *To Peng*: Thank you for your help in Shanghai. I am quite fond of Chinese food, Chinese hospitality and Chinese speed!
- *To Heeralal*: Thank you for your time. It has been one of the most valuable things that I have been given.
- *To all my DTU colleagues*: Thank you for making the institute a comfortable work place. It was a good place to be in. In particular: Johan, thank you for showing me Danish hospitality and making Office 153 a "hygge" office.

Contents

Chapter 1

Introduction

Graph based codes, and affine variety codes, are code constructions. As such, each code gives a different perspective in coding theory. The graph based code construction boils down to building a long code starting with several short codes, and a graph which describes how to join the shorter codes together to build up the longer code one wants. The choice of code and graph to construct the long graph code gives some information about the resulting code parameters. This information is not complete, as the graph based code construction gives a wide leeway to construct a graph code from a graph and a code. What makes graph codes tantalizing for implementation is that the graph based code construction gives a simple and fast decoding algorithm based only on the graph and the decoder of the component code. This is where most research of graph based codes is focused, on minimum distance and decoding. Usually, research on graph based codes focuses on the class of codes defined by a graph and a component code, but our research focuses on specific graph based codes in order to understand the dimension of graph based codes.

When Tanner introduced graph based codes he remarked that any code could be described as a graph based code construction. This is why we say graph based codes are also a perspective on coding theory. Here we study codes from the perspective of both graph based codes and affine variety codes.

In the second chapter, we introduce: polynomial rings, ideals, varieties, Gröbner

bases, polynomial functions and other concepts in order to define affine variety codes with the required mathematical background. Most of the material is standard, although we also present theorems specifically for our work on graph based codes. We finish the second chapter with some examples of affine variety codes in order to familiarize the reader.

After laying the groundwork on affine variety codes in the third chapter, we introduce: bipartite graphs, labelings and two constructions of graph based codes, Tanner codes and graph codes. In this thesis, we have omitted another well–known class of graph based codes known as expander codes. Introducing expander codes would have complicated our exposition to the topic severly. Nonetheless, for those interested in expander codes, they are also constructed as Tanner codes in a simple and intuitive way. When Tanner introduced graph based codes he also remarked upon the similarity between the two constructions we present. We make this similarity rigourous in order to use a original result on graph codes to get the dimension of some Tanner codes. We finish the third chapter with some examples of graph codes and Tanner codes.

After presenting the required background, we begin making graph based codes as affine variety codes. In the fourth chapter, we present some Tanner codes with cyclic component codes. After the necessary background on subfield subcodes we describe the underlying graph as an affine variety. Then, we use some cyclic component codes such that the graph codes are generated by rational functions over the affine variety representing the graph. Then, we present some improvements to compute the dimension for the graph based codes with cyclic component codes. From this improvement, we present the dimension for some of these graph codes with cyclic component codes. Since Tanner codes are also a graph codes with cyclic component codes, we present some Tanner codes from the same construction which turn out to have maximal or best known parameters.

The fifth chapter consists of studying graph based codes with Reed–Solomon component codes. We present the graph codes from two different graphs with the same Reed–Solomon component codes. As in chapter four, we present the underlying graphs as an affine variety. Then, we present the graph codes as affine variety codes over the graphs. With Reed–Solomon codes, and as opposed to chapter four, we can find explicit bounds for the graph code dimension in this case. We prove when the formulas are exact and give examples when the formulas fail.

In last chapter, we study Grassmann codes and affine Grassmann codes. Affine Grassmann codes are defined as affine variety codes. From the minimum distance codewords of their dual code, we prove affine Grassmann codes are Tanner codes with other affine Grassmann codes as component codes. Since Tanner code

is also described in terms of the puncturing and shortening operations, we can also view Grassmann codes as Tanner codes with other Grassmann codes as component codes.

Now we present some preliminary notions of coding theory of interest for us.

1.1 Coding Theory Notions

Definition 1.1.1 *For* $\boldsymbol{x} = (x_1, x_2, \ldots, x_n), \boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathbf{F}^n$, *we define* Hamming distance *between* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *as*

$$d(\boldsymbol{x}, \boldsymbol{y}) := \#\{i \mid x_i \neq y_i,\ i = 1, 2, \ldots n\}.$$

Definition 1.1.2 *For* $S \subseteq \mathbf{F}^n$ *we define the minimum distance of* S *as*

$$d(S) := \min_{\boldsymbol{x} \neq \boldsymbol{y} \in S} d(\boldsymbol{x}, \boldsymbol{y}).$$

Definition 1.1.3 *Let* C *be an* $\mathbf{F}_q$*-linear subspace of* $\mathbf{F}_q^n$. *Then* C *is a* (linear) code *over* $\mathbf{F}_q$. *The parameters of* C *are the length* n, *the dimension* $\dim_{\mathbf{F}_q} C$ *and* $d(C)$. *If* $\dim_{\mathbf{F}_q} C = k$ *and* $d(C) = d$, *then we say* C *is a* $[n, k, d]_{\mathbf{F}_q}$ *code. If we wish to emphasize only the field* $\mathbf{F}_q$, *then we say* C *is a code over* $\mathbf{F}_q$. *If* $\boldsymbol{c} \in C$ *then* $\boldsymbol{c}$ *is a* codeword *of* C.

Lemma 1.1.4 *Let* C *be a linear code over* $\mathbf{F}_q$. *If* $\boldsymbol{c}, \boldsymbol{c}'$ *are two codewords of* C *of minimum weight and on the same nonzero coordinates, then* $\boldsymbol{c}' = \alpha \boldsymbol{c}$ *for some* $\alpha \in \mathbf{F}_q^*$.

Proof.

Let $c'_i = \alpha c_i \neq 0$. Then the vector $\mathbf{c}' - \alpha \mathbf{c}$ is a codeword of C with a weight strictly less than $d(C)$. Therefore, $\mathbf{c}' - \alpha \mathbf{c}$ must be the zero codeword. □

Although, there exist nonlinear codes, we consider only codes which are linear subspaces of $\mathbf{F}_q^n$. Hereafter, linear codes will be referred to as codes. Since we are working with linear spaces, we have the following definitions.

Definition 1.1.5 *Let* C *be a code of length* n *and dimension* k *over* $\mathbf{F}_q$. *An* generator matrix for C *is an* $k \times n$ *matrix* G *over* $\mathbf{F}_q$ *whose rowspace is* C.

The generator matrix for a code gives a compact way to describe a code and its dual. If G is the generator matrix of C, then $C^\perp$ is the right nullspace of G.

Definition 1.1.6 *Let C be an $\mathbf{F}_q$-linear subspace of $\mathbf{F}_q^n$. We define the* dual code *of C as the orthogonal complement of C. That is*

$$C^\perp := \{\boldsymbol{x} \in \mathbf{F}_q^n \mid \forall \boldsymbol{c} \in C \; x_1c_1 + x_2c_2 + \cdots + x_nc_n = 0\}.$$

The code $C^\perp$ is a $[n, n-k, d(C^\perp)]_{\mathbf{F}_q}$ code.

Definition 1.1.7 *Let C_1, C_2 be codes of length n over $\mathbf{F}_q$. We say C_1 and C_2 are* monomially equivalent codes *if there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{F}_q^*$ such that*

$$(c_1, c_2, \ldots, c_n) \in C_1 \text{ if and only if } (\alpha_1c_1, \alpha_2c_2, \ldots, \alpha_nc_n) \in C_2.$$

And we have the following theorem.

Theorem 1.1.8 *Suppose C_1 and C_2 are monomially equivalent codes. Then $C_1^\perp$ is monomially equivalent to $C_2^\perp$.*

Now we present another notion of equivalent codes based on permutations.

Definition 1.1.9 *Let C be a code of length n. Suppose σ is a permutation of $\{1, 2, \ldots, n\}$. If $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$, then $\sigma(\boldsymbol{c}) := (c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)})$. We also define $\sigma(C) := \{\sigma(c) \mid c \in C\}$. In case $\sigma(C) = C$, then σ is called an* automorphism of C. *The group of all automorphisms is denoted by $Aut(C)$.*

Note that if C is a code, then $\sigma(C)$ is a code with the same parameters as C.

Definition 1.1.10 *If a code D is obtained by permuting the positions of a code C, then the code D is* permutation equivalent *to C. We denote it by $C \equiv D$.*

Definition 1.1.11 *Let C be a code of length n over $\mathbf{F}_q$. Suppose the set $I = \{i_1, i_2, \ldots, i_m\}$ is a subset of the code positions $\{1, 2, \ldots, n\}$. We define the* punctured code of C at I *as*

$$C^I := \{(c_{i_1}, c_{i_2}, \ldots, c_{i_m}) \in \mathbf{F}_q^I \mid \boldsymbol{c} \in C\}.$$

We also define the shortened code of C at I *as*

$$C_I := \{(c_{i_1}, c_{i_2}, \ldots, c_{i_m}) \in \mathbf{F}_q^I \mid \boldsymbol{c} \in C, c_i = 0, i \notin I\}.$$

Note that puncturing a code means discarding all the coordinates outside of I and shortening means to set all coordinates outside of I equal to 0, and then discarding these. Mathematically puncturing a code C on the positions given by I is projecting the code onto the positions given by I. In coding theory puncturing is usually reserved for the case the dimension does not decrease. We use either term. We have the following theorem.

Theorem 1.1.12 *Let C be a code of length n over $\mathbf{F}_q$. Let $I = \{i_1, i_2, \ldots, i_m\}$ be a subset of the positions of C, then*

$$(C^\perp)^I = (C_I)^\perp.$$

Puncturing and shortening codes are an elementary way of constructing codes from longer codes. In addition, puncturing and shortening also give some control of the parameters of the punctured code in terms of the parameters of the original code. These two concepts are also important in undestanding graph based codes.

Definition 1.1.13 *Let C be a code of length n over $\mathbf{F}_q$ and dimension k. An* information set of C *is a subset, I_C, of k positions of C such that the submatrix of the generator matrix of G obtained from the columns of I_C has full rank.*

An equivalent definition of an information set of C is a set of coordinates such that the values of a codeword at the coordinates of the information set determine the codeword uniquely. Therefore, the information set is a set which has all the information about a codeword. Once the entries in an information set have been determined, then all other entries are also determined. Note that, for a code of dimension k there exists at least one information set of size k,

Theorem 1.1.14 (The Singleton bound) *Let C be an $[n, k, d]$ code. Then,*

$$d \leq n - k + 1.$$

In coding theory one of the most important class of codes are those for the Singleton bound holds with equality. That is:

Definition 1.1.15 An MDS code *is an* $[n, k, d]$ *code which satisfies the Singleton bound with equality. That is:*

$$d = n - k + 1.$$

MDS is short for Maximum Distance Separable. There are several characterizations of MDS codes. We can relate MDS codes to the other concepts we have introduced in the following theorem:

Theorem 1.1.16 *Let* C *be an* $[n, k, d]$ *code. Let* I *be a subset of* n' *coordinates of* C*. The following are equivalent:*

- C *is an MDS code.*
- $C^{\perp}$ *is an MDS code.*
- *Any set of* k *coordinates of* C *is an information set for* C*.*
- *Any puncturing of* C *(including* C *itself) is an MDS code.*
- *Any shortening of* C *(including* C *itself) is an MDS code.*

1.2 What is a good code?

Graph based codes were introduced by Gallagher in [Gal63]. Later, Tanner also worked on graph based codes starting in [Tan81]. After these seminal works, others have also worked on graph based codes, such as Low Density Parity Check (LDPC) codes and Expander codes. Some significant articles are: [ABN+92, Zem01, KLF01, SS96, BZ05, RS06].

The allure of graph codes is that their performance as a good code does not depend on their minimum distance, instead it depends on the performance of the iterative decoder. Normally, the minimum distance of a code is a proxy for good decoding performance. However, some LDPC codes, Expander codes and Product codes decode much better than what their minimum distance predicts. Tanner in [Tan84] shows that the decoding and minimum distance of a graph based code depends on the second largest eigenvalue of the graphs. The decoding performance actually depends on the expansion of the graph. Expander graphs are studied in [Alo86, DBL84, Mar88, Nil91, Mor94, LU95].

Good codes with good decoding performance using the graph expansion property are studied in [GI01, GI02, RU01a, RU01b, RSU01, SR03, LRC08].

Chapter 2

Affine Variety Codes

Our algebraic approach to graph based codes is based on affine varieties. By treating both the graphs and the component codes within the same framework of affine varieties, we can construct some graph based codes under the same framework. In this chapter, we introduce affine variety codes. With affine varieties, we study codes from algebraic objects such as curves and surfaces. These algebraic objects add an extra algebraic layer to coding theory. We describe affine varieties with polynomial rings, ideals and Gröbner bases. The material and notation follows [CLO07] closely.

This chapter is organized as follows. First, we introduce polynomial rings. Second, we introduce ideals and Gröbner bases. Third, we introduce ideals of polynomial rings and affine varieties. Lastly, we introduce affine variety codes and give some examples.

2.1 Polynomial Rings

Definition 2.1.1 *A* monomial *in $x_1, x_2, \ldots, x_n$ is a product of the form*

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}, \text{ where } a_1, a_2, \ldots, a_n \in \mathbb{N}.$$

We may simplify the notation of $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ *to* $x^{\boldsymbol{a}}$. *The* total degree *of the monomial is* $a_1 + a_2 + \cdots + a_n$. *We denote the total degree as* $deg(x^{\boldsymbol{a}})$.

Definition 2.1.2 *Let* $\mathbf{k}$ *be a field. A* polynomial *in* $\mathbf{k}$ *is a finite,* $\mathbf{k}$*-linear combination of monomials. We can write a polynomial* f *in the form*

$$f = \sum_{\boldsymbol{a}} f_{\boldsymbol{a}} x^{\boldsymbol{a}}, f_{\boldsymbol{a}} \in \mathbf{k}$$

where the sum is over a finite number of vectors $\boldsymbol{a} \in \mathbb{N}^n$. *The set of all polynomials in* $x_1, x_2, \ldots, x_n$ *with coefficients in* $\mathbf{k}$ *is denoted by* $\mathbf{k}[x_1, x_2, \ldots, x_n]$.

We can make the polynomial ring $\mathbf{k}[x_1, x_2, \ldots, x_n]$ into a domain with the following addition and multiplication operations.

Theorem 2.1.3 *Suppose that the product of* $x^{\boldsymbol{a}}$ *and* $x^{\boldsymbol{b}}$ *is* $x^{\boldsymbol{a}+\boldsymbol{b}}$. *In addition, let* $f = \sum_{\boldsymbol{a}} f_{\boldsymbol{a}} x^{\boldsymbol{a}}$ *and* $g = \sum_{\boldsymbol{a}} g_{\boldsymbol{a}} x^{\boldsymbol{a}}$ *be polynomials in* $\mathbf{k}[x_1, x_2, \ldots, x_n]$. *Then, the ring* $\mathbf{k}[x_1, x_2, \ldots, x_n]$ *is a domain with the operations*

$$f + g := \sum_{\boldsymbol{a}} (f_{\boldsymbol{a}} + g_{\boldsymbol{a}}) x^{\boldsymbol{a}}, \text{ and } fg := \sum_{\boldsymbol{a}} \Big(\sum_{\boldsymbol{b}+\boldsymbol{c}=\boldsymbol{a}} f_{\boldsymbol{b}} g_{\boldsymbol{c}} \Big) x^{\boldsymbol{a}}.$$

Definition 2.1.4 *Let* $f = \sum_{\boldsymbol{a}} f_{\boldsymbol{a}} x^{\boldsymbol{a}}$ *be a polynomial in* $\mathbf{k}[x_1, x_2, \ldots, x_n]$. *The element* $f_{\boldsymbol{a}} \in \mathbf{k}$ *is the* coefficient *of* $x^{\boldsymbol{a}}$ *in* f. *If* $f_{\boldsymbol{a}} \neq 0$, *then* $f_{\boldsymbol{a}} x^{\boldsymbol{a}}$ *is a* term *of* f. *The* total degree *of* f *is the highest total degree among the monomials of the terms of* f. *We denote the total degree of* f *by* $deg(f)$.

2.2 Ideals and Gröbner bases

Gröbner bases are important computational tools when working with ideals in polynomial rings. These bases contain the information necessary to answer some fundamental questions about a polynomial ring ideal quickly and easily. Ideals and Gröbner bases are elementary tools to study affine variety codes.

Definition 2.2.1 *A subset* $I \subset \mathbf{k}[x_1, x_2, \ldots, x_n]$ *is an* ideal *of the polynomial ring* $\mathbf{k}[x_1, x_2, \ldots, x_n]$ *if it satisfies the following:*

- *If* $f, g \in I$ *then* $f + g \in I$.
- *If* $f \in I$ *and* $h \in \mathbf{k}[x_1, x_2, \ldots, x_n]$ *then* $fh \in I$.

Definition 2.2.2 *Let $f_1, f_2, \ldots, f_s \in \mathbf{k}[x_1, x_2, \ldots, x_n]$. We define*

$$\langle f_1, f_2, \ldots, f_s \rangle := \{\sum_{i=1}^{s} h_i f_i \mid h_i \in \mathbf{k}[x_1, x_2, \ldots, x_n]\}.$$

With the definition of an ideal and the definition of $\langle f_1, f_2, \ldots, f_s \rangle$ one can easily work out that $\langle f_1, f_2, \ldots, f_s \rangle$ is an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. Thus, we call the ideal $\langle f_1, f_2, \ldots, f_s \rangle$ the ideal generated by $f_1, f_2, \ldots, f_s$.

Definition 2.2.3 *A* monomial order, $\preceq$, *is a total ordering on the monomials on $x_1, x_2, \ldots, x_n$ such that:*

- $1 \preceq x^{\boldsymbol{a}}$ *for all monomials* $x^{\boldsymbol{a}}$.
- *For all monomials* $x^{\boldsymbol{a}}$ *and* $x^{\boldsymbol{b}}$ *if* $x^{\boldsymbol{b}} \preceq x^{\boldsymbol{a}}$ *and* $x^{\boldsymbol{a}} \preceq x^{\boldsymbol{b}}$ *hold then* $x^{\boldsymbol{a}} = x^{\boldsymbol{b}}$.
- *For all monomials* $x^{\boldsymbol{a}}$, $x^{\boldsymbol{b}}$ *and* $x^{\boldsymbol{c}}$ *if* $x^{\boldsymbol{a}} \preceq x^{\boldsymbol{b}}$ *then* $x^{\boldsymbol{a}+\boldsymbol{c}} \preceq x^{\boldsymbol{b}+\boldsymbol{c}}$.

For a monomial order $\preceq$, the relation $x^{\mathbf{a}} \preceq x^{\mathbf{b}}$ includes the possibility $x^{\mathbf{a}} = x^{\mathbf{b}}$. The relation $x^{\mathbf{a}} \prec x^{\mathbf{b}}$ is equivalent to $x^{\mathbf{a}} \preceq x^{\mathbf{b}}$ but $x^{\mathbf{a}} \neq x^{\mathbf{b}}$.

Definition 2.2.4 *For monomials* $x^{\boldsymbol{a}}$ *and* $x^{\boldsymbol{b}}$ *on* $x_1, x_2, \ldots, x_n$, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}^n$ *we define the* lexicographical order, $\leq_{lex}$ *with* $x_1 > x_2 > \cdots > x_n$ *as follows.*

If $a_1 = b_1, a_2 = b_2, \cdots, a_{i-1} = b_{i-1}$ *but* $a_i < b_i$, *then* $x^{\boldsymbol{a}} <_{lex} x^{\boldsymbol{b}}$.

For monomials $x^{\boldsymbol{a}}$ *and* $x^{\boldsymbol{b}}$ *on* $x_1, x_2, \ldots, x_n$, $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{N}^n$ *we define the* degree graded lexicographical order, $\leq_{glex}$, *with* $x_1 > x_2 > \cdots > x_n$ *as follows:*

$x^{\boldsymbol{a}} <_{glex} x^{\boldsymbol{b}}$ *if and only if* $deg(\boldsymbol{a}) < deg(\boldsymbol{b})$ *or* $deg(\boldsymbol{a}) = deg(\boldsymbol{b})$ *and* $x^{\boldsymbol{a}} <_{lex} x^{\boldsymbol{b}}$,

where $\leq_{lex}$ *is the lexicographical order with* $x_1 > x_2 > \cdots > x_n$.

The degree graded reverse lexicographical order, $\leq_{grlex}$ *with* $x_1 > x_2 > \cdots > x_n$ *is defined as*

$x^{\boldsymbol{a}} <_{grlex} x^{\boldsymbol{b}}$ *if and only if* $deg(\boldsymbol{a}) < deg(\boldsymbol{b})$ *or* $deg(\boldsymbol{a}) = deg(\boldsymbol{b})$ *and* $x^{\boldsymbol{a}} >_{rlex} x^{\boldsymbol{b}}$

where $\leq_{rlex}$ *is the lexicographical order with* $x_n > x_{n-1} > \cdots > x_2 > x_1$.

Definition 2.2.5 *Let* $f = \sum_{\boldsymbol{a}} f_{\boldsymbol{a}} x^{\boldsymbol{a}}$ *be a polynomial in* $\mathbf{k}[x_1, x_2, \ldots, x_n]$. *Let* $\preceq$ *be a monomial order among the monomials in* $x_1, x_2, \ldots, x_n$ *If* $x^{\boldsymbol{a}}$ *is the greatest monomial among all terms of* f, *then* $f_{\boldsymbol{a}}$ *is the* leading coefficient *of* f *under* $\preceq$, $x^{\boldsymbol{a}}$ *is the* leading monomial *of* f *under* $\preceq$ *and* $f_{\boldsymbol{a}} x^{\boldsymbol{a}}$ *is the* leading term *of* f *under* $\preceq$. *We denote the leading term of* f *by* $LT_{\preceq}(f)$, *the leading coefficient by* $LC_{\preceq}(f)$ *and the leading monomial by* $LM_{\preceq}(f)$.

The fundamental algorithm in computations with ideals in a polynomial ring is the multivariate polynomial division algorithm.

Algorithm 1 *Multivariate division algorithm in* $\mathbf{k}[x_1, x_2, \ldots, x_n]$ *under* $\preceq$

Input: $f_1, f_2, \ldots, f_s, f$.
Output: $a_1, a_2, \ldots, a_s, r$.
$a_1 := 0, a_2 := 0, \ldots, a_s := 0, r := 0$
$p := f$
while $p \neq 0$ ***do***
  $i := 1$
  $divisionoccurred := FALSE$
  while $i \leq s$ *and* $divisionoccurred = FALSE$ ***do***
    if $LM_{\preceq}(f_i)$ *divides* $LM_{\preceq}(p)$ ***then***
      $a_i := a_i + \frac{LT_{\preceq}(p)}{LT_{\preceq}(f_i)}$
      $p := p - \frac{LT_{\preceq}(p)}{LT_{\preceq}(f_i)} f_i$
      $divisionoccurred := TRUE$
    else
      $i := i + 1$
    end if
  end while
  if $divisionoccurred = FALSE$ ***then***
    $r := r + LT_{\preceq}(p)$
    $p := p - LT_{\preceq}(p)$
  end if
end while

end

Definition 2.2.6 *The output* r *when dividing* f *by* $f_1, f_2, \ldots, f_s$ *is called the* remainder of f when divided by $f_1, f_2, \ldots, f_s$. *The outputs* $a_1, a_2, \ldots, a_s$ *are known as the* quotients.

Theorem 2.2.7 *Fix a monomial order* $\preceq$. *Let* $F = (f_1, f_2, \ldots, f_s)$ *be an* s*-tuple of polynomials in* $\mathbf{k}[x_1, x_2, \ldots, x_n]$. *For any* $f \in \mathbf{k}[x_1, x_2, \ldots, x_n]$ *there exist* $a_i, r \in \mathbf{k}[x_1, x_2, \ldots, x_n]$ *such that,*

- $f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$,
- *none of the terms of* r *are divisible by any of the monomials* $LM_{\preceq}(f_i)$,
- *and if* $a_i f_i \neq 0$ *then* $LM_{\preceq}(a_i f_i) \preceq LM_{\preceq}(f)$.

PROOF.

The output of the multivariate division algorithm in $\mathbf{k}[x_1, x_2, \ldots, x_n]$, when the input is $f_1, f_2, \ldots, f_s, f$, satisfies the conclusion of the theorem. □

DEFINITION 2.2.8 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. Let $\preceq$ be a monomial order. We define $LM_{\preceq}(I)$ as the set of leading monomials of the polynomials in I, that is*

$$LM_{\preceq}(I) := \{x^{\boldsymbol{a}} \mid \exists\ f \in I\ :\ LM_{\preceq}(f) = x^{\boldsymbol{a}}\}.$$

DEFINITION 2.2.9 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. We define*

$$\Delta_{\preceq}(I) := \{x^{\boldsymbol{a}} \mid x^{\boldsymbol{a}} \notin LM_{\preceq}(I)\}.$$

The set $\Delta_{\preceq}(I)$ is a normal basis *for $\mathbf{k}[x_1, x_2, \ldots, x_n]/I$ under $\preceq$. This is also known as the* footprint of I. *This term was introduced by R.E. Blahut.*

We call $\Delta_{\preceq}(I)$ a normal basis because of the following:

THEOREM 2.2.10 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. Suppose $\preceq$ is a monomial order. Then $\{x^{\boldsymbol{a}} + I \mid x^{\boldsymbol{a}} \in \Delta_{\preceq}(I)\}$ is a basis for $\mathbf{k}[x_1, x_2, \ldots, x_n]/I$ as a $\mathbf{k}$-vector space.*

The sets $LM_{\preceq}(I)$ and $\Delta_{\preceq}(I)$ contain plenty of information about the ideal I. For example, $I \cap Span_{\mathbf{k}}(\Delta_{\preceq}(I)) = \{0\}$. Also, if we know a basis for the ideal I from which the set $LM_{\preceq}(I)$ is easily derived then we can easily determine whether or not a polynomial belongs to the ideal.

DEFINITION 2.2.11 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. Let $\preceq$ be a monomial order. The set $\{g_1, g_2, \ldots, g_m\}$ is a* Gröbner basis *for I under $\preceq$ if and only if the following hold:*

- $\langle g_1, g_2, \ldots, g_m\rangle = I$,
- $\langle LM_{\preceq}(g_1), LM_{\preceq}(g_2), \ldots, LM_{\preceq}(g_m)\rangle = \langle LM_{\preceq}(I)\rangle$.

With a Gröbner basis for I under $\preceq$ we can derive $\Delta_{\preceq}(I)$ easily. The next theorem expands upon the usefulness of Gröbner bases.

THEOREM 2.2.12 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. Let $\preceq$ be a monomial order. Suppose $\langle g_1, g_2, \ldots, g_m\rangle = I$. The following are equivalent:*

- *The basis* $\{g_1, g_2, \ldots, g_m\}$ *is a Gröbner basis for* I *under* $\preceq$,
- *The remainder of any* f *when divided by* $g_1, g_2, \ldots, g_m$ *is equal to the remainder when* f *is divided by any permutation of* $g_1, g_2, \ldots, g_m$,
- *The remainder of any* $f \in I$ *when divided by* $g_1, g_2, \ldots, g_m$ *is* 0.

The Gröbner basis is the key to compute in $\mathbf{k}[x_1, x_2, \ldots, x_n]/I$. The remainder when dividing by a Gröbner basis under $\preceq$ will always belong to $Span_{\mathbf{k}}(\Delta_{\preceq}(I))$. If we divide f by a Gröbner basis of I under $\preceq$, we denote the remainder by $rem_{\preceq}(f)$.

2.3 Affine Varieties and Ideals

Definition 2.3.1 *We define the* n*-dimensional affine space of* $\mathbf{k}$ *as*

$$\mathbb{A}(n, \mathbf{k}) := \{(p_1, p_2, \ldots, p_n) \mid \forall i = 1, 2, \ldots, n \ : \ p_i \in \mathbf{k}\}.$$

The elements of $\mathbb{A}(n, \mathbf{k})$ *are also known as points. The affine space* $\mathbb{A}(1, \mathbf{k})$ *is known as the affine line and* $\mathbb{A}(2, \mathbf{k})$ *is known as the affine plane.*

Definition 2.3.2 *Let* $f \in \mathbf{k}[x_1, x_2, \ldots, x_n]$. *Let* $\boldsymbol{p}$ *be a point of* $\mathbb{A}(n, \mathbf{k})$. *If we replace* x_i *by* p_i *then we obtain an element of* $\mathbf{k}$ *defined as the evaluation of* f *at* $\boldsymbol{p}$ *denoted by either* $f(p_1, p_2, \ldots, p_n)$ *or* $f(\boldsymbol{p})$. *In this way,* f *gives rise to a* polynomial function *from* $\mathbb{A}(n, \mathbf{k})$ *to* $\mathbf{k}$. *The polynomial function given by* f *is also denoted by* f.

Lemma 2.3.3 *Let* $\mathbf{k}$ *be a field with an infinite number of elements. The only polynomial which evaluates to* 0 *on all points of* $\mathbb{A}(n, \mathbf{k})$ *is* 0.

Please note, it is important that the field $\mathbf{k}$ has an infinite number of elements. Over $\mathbf{F}_q$, the nonzero polynomial $x^q - x$ gives the zero function in $\mathbb{A}(1, \mathbf{F}_q)$.

Definition 2.3.4 *We denote by* $\bar{\mathbf{k}}$ *a fixed algebraic closure of the field* $\mathbf{k}$.

Definition 2.3.5 *Let* $f_1, f_2, \ldots, f_s \in \mathbf{k}[x_1, x_2, \ldots, x_n]$. *We define*

$$\boldsymbol{V}(f_1, f_2, \ldots, f_s) := \{\boldsymbol{p} \in \mathbb{A}(n, \mathbf{k}) \mid \forall \ i \ : \ f_i(\boldsymbol{p}) = 0\}.$$

The set $\boldsymbol{V}(f_1, f_2, \ldots, f_s)$ *is the* affine variety over $\mathbf{k}$ *defined by* $f_1, f_2, \ldots, f_s$.

This definition of an affine variety is not the standard definition. The object we are defining technically is the zero locus of a set of polynomials. Affine varieties are also geometrical objects and we want to use this to construct to our liking. Now we define several relations between ideals and affine varieties. With these we may switch between algebraic and geometric descriptions, making them essential to algebraic geometry.

Definition 2.3.6 *Let $V \subseteq \mathbb{A}(n, \mathbf{k})$ be an affine variety. We define $\boldsymbol{I}(V)$ as*

$$\boldsymbol{I}(V) := \{f \in \mathbf{k}[x_1, x_2, \ldots, x_n] \mid \forall\ \boldsymbol{p}\ \in V\ :\ f(\boldsymbol{p}) = 0\ \}.$$

Clearly, $\boldsymbol{I}(V)$ is an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. The ideal $\boldsymbol{I}(V)$ is called the ideal of the variety V .

Definition 2.3.7 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. We define*

$$\boldsymbol{V}(I) := \{\boldsymbol{p} \in \mathbb{A}(n, \mathbf{k}) \mid f(\boldsymbol{p}) = 0\ \forall f \in I\}.$$

Since any ideal I is generated by some $f_1, f_2, \ldots, f_s \in \mathbf{k}[x_1, x_2, \ldots, x_n]$, we can write $\mathbf{V}(I) = \mathbf{V}(f_1, f_2, \ldots, f_s)$. Thus $\mathbf{V}(I)$ is an affine variety.

Definition 2.3.8 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. The ideal I is a* radical ideal *if $f^m \in I$ for some m implies $f \in I$.*

Definition 2.3.9 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$. The* radical ideal of *I is denoted by $\sqrt{I}$ and defined as*

$$\sqrt{I} := \{f \mid \exists\ m \in \mathbb{N} : f^m \in I\}.$$

From the definition one can easily prove that $\sqrt{I}$ is a radical ideal.

Lemma 2.3.10 *If V is an affine variety, then $\boldsymbol{I}(V)$ is a radical ideal.*

We have defined ideals, varieties, the ideal of a variety and the variety of an ideal. We know that the ideal of a variety is radical. The next theorems tell us more about the nature of this mapping between ideals and varieties and how to find a 1-1 correspondence between some ideals and varieties.

Theorem 2.3.11 (The Nullstellensatz) *Let I be an ideal of the polynomial ring $\bar{\mathbf{k}}[x_1, x_2, \ldots, x_n]$. Then,*

$$\boldsymbol{I}(\,\boldsymbol{V}(I)) = \sqrt{I}.$$

Theorem 2.3.12 (Ideal–Variety Correspondence) *For any field* $\mathbf{k}$ *and an affine variety* $V \subseteq \mathbb{A}(n, \mathbf{k})$ *we have*

$$V = \boldsymbol{V}(\boldsymbol{I}(V)).$$

Moreover, for $\mathbf{k} = \bar{\mathbf{k}}$ *and for a radical ideal* $I \subseteq \mathbf{k}[x_1, x_2, \ldots, x_n]$ *we also have*

$$I = \boldsymbol{I}(\boldsymbol{V}(I)).$$

The Ideal–Variety correspondence theorem is the fundamental relation between ideals and affine varieties. With this algebraic geometrical relation, we may define polynomial functions on a affine variety. Later on, we will define affine variety codes with these polynomial functions.

Definition 2.3.13 *For a field* $\mathbf{k}$ *and* V *an affine variety of* $\mathbb{A}(n, \mathbf{k})$*, we denote by* $\mathbf{k}[V]$ *the ring of all polynomial functions from* V *to* $\mathbf{k}$*.*

Theorem 2.3.14 *Let* $f, g \in \bar{\mathbf{k}}[x_1, x_2, \ldots, x_n]$*. Let* V *be an affine variety of* $\mathbb{A}(n, \bar{\mathbf{k}})$*. Then,* f *and* g *represent the same polynomial function in* $\bar{\mathbf{k}}[V]$ *if and only if* $f - g \in \boldsymbol{I}(V)$*.*

The next corollary shows the relation between the polynomial functions over an affine variety V and the quotient ring $\bar{\mathbf{k}}[x_1, x_2, \ldots, x_n]/\mathbf{I}(V)$.

Corollary 2.3.15 *Let* $\bar{\mathbf{k}}[x_1, x_2, \ldots, x_n]$ *be a polynomial ring,* V *any affine variety of* $\mathbb{A}(n, \bar{\mathbf{k}})$*. Then* $\bar{\mathbf{k}}[V]$ *and* $\bar{\mathbf{k}}[x_1, x_2, \ldots, x_n]/\boldsymbol{I}(V)$ *are isomorphic rings.*

Note that since the Nullstellensatz holds only for algebraically closed fields, we may not be able to apply Corollary 2.3.15 for any field. In the next subsection, we study a case where Corollary 2.3.15 holds over non algebraically closed fields.

2.3.1 Finite Affine Varieties

Theorem 2.3.16 *Let* I *be an ideal of* $\mathbf{k}[x_1, x_2, \ldots, x_n]$*, such that,* $\boldsymbol{V}(I)$ *is a finite set. Then*

- $\#\,\boldsymbol{V}(I)$ *is at most* $\dim \mathbf{k}[x_1, x_2, \ldots, x_n]/I$*.*
- *If* I *is a radical ideal then equality holds;* $\dim \mathbf{k}[x_1, x_2, \ldots, x_n]/I = \#\,\boldsymbol{V}(I)$*.*

- *For each x_i there is a univariate polynomial $f_i(x_i) \in I$. If the degree of $f_i(x_i)$ is m_i then $\#\boldsymbol{V}(I) \leq m_1 m_2 \cdots m_n$.*

From [GH00] the first bound is referred to as the *footprint bound*. Now we improve the footprint bound.

Theorem 2.3.17 *Let I be an ideal of $\mathbf{k}[x_1, x_2, \ldots, x_n]$, such that, $\boldsymbol{V}(I)$ is a finite set. Let $g_1, g_2, \ldots, g_s$ be a basis of I. Then, for a monomial order $\preceq$ the following holds:*

$$\#\Delta_{\preceq}(I) \leq \#\Delta_{\preceq}(\ \langle LM_{\preceq}(g_1), LM_{\preceq}(g_2), \ldots, LM_{\preceq}(g_s)\rangle)$$

with equality if and only if $g_1, g_2, \ldots, g_s$ is a Gröbner basis for I under $\preceq$.

We need a particular lemma on ideals and polynomials of the form $x_i^q - x_i$.

Lemma 2.3.18 *Let I be an ideal of $\mathbf{F}_q[x_1, x_2, \ldots, x_n]$. Suppose that for each x_i there is a univariate polynomial $x_i^q - x_i \in I$. Then I is radical.*

Lemma 2.3.18 is a specific instance of Seidenberg's lemma. [Sei74]

Our interest on Affine Variety codes is based on affine varieties over $\mathbf{F}_q$. Now we show that we can work with ideals over $\mathbf{F}_q$. To do this, we state an explicit basis of the ideal of any affine variety of $\mathbb{A}(n, \mathbf{F}_q)$. We begin with a definition of interpolating polynomials.

Definition 2.3.19 *Let $\boldsymbol{p} = (p_1, p_2, \ldots, p_n)$ be a point of $\mathbb{A}(n, \mathbf{F}_q)$. The* characteristic polynomial of $\mathbf{p}$ over $\mathbf{F}_q$ *is the polynomial*

$$F_{\boldsymbol{p}} := 1 - \prod_{i=1}^{n} (1 - (x_i - p_i)^{q-1}).$$

If V is a set of points of $\mathbb{A}(n, \mathbf{F}_q)$ we define the characteristic polynomial of V over $\mathbf{F}_q$ *as the polynomial*

$$F_V := \prod_{\boldsymbol{p} \in V} F_{\boldsymbol{p}}.$$

This interpolating polynomial is not the Lagrange interpolation polynomial. Rather we are making a polynomial whose zeroes in $\mathbb{A}(n, \mathbf{F}_q)$ are exactly the point of the affine variety V. We describe it as follows.

Lemma 2.3.20 *If $\boldsymbol{p}$ is a point of $\mathbb{A}(n, \mathbf{F}_q)$, then $F_V(\boldsymbol{p}) = 0$ if and only if $\boldsymbol{p} \in V$.*

Theorem 2.3.21 *Let V be a finite set of points of $\mathbb{A}(n, \mathbf{F}_q)$. Suppose f is a polynomial whose zeroes over $\mathbb{A}(n, \mathbf{F}_q)$ are V. Then, V is the affine variety $\boldsymbol{V}(x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n, f)$. Moreover, the ideal $\boldsymbol{I}(V)$ is generated by $\langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n, f \rangle$.*

Proof.

Let $J := \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n, f \rangle$. Since $x_i^q - x_i$ belongs to J, the points of the variety $V(J)$ are contained in $\mathbb{A}(n, \mathbf{F}_q)$. Furthermore, only the zeroes of f may belong to $V(J)$. Therefore $V(J)$ as a variety of $\mathbb{A}(n, \bar{\mathbf{F}}_\mathbf{q})$ is V. This implies $J \subseteq \mathbf{I}(V)$. Since $x_i^q - x_i$ belongs to J, Seidenberg's lemma implies J is radical. The Nullstellensatz implies equality. □

2.3.2 Footprint bound examples

We show some examples in which we use the footprint bound to find the Gröbner basis of some affine varieties of $\mathbb{A}(n, \mathbf{F}_q)$. These examples are relevant for the graph codes we will present later on.

Example 2.3.22 *Consider $V = \{(x, y, a, b) \in \mathbf{F}_q^4 \mid ax + b - y = 0\}$. This set is an affine variety of $\mathbb{A}(4, \mathbf{F}_q)$. From the definition of V, we may choose the values of x, y and a without any restrictions, but b is uniquely determined. Therefore, $\#V = q^3$. Suppose I is the ideal generated by $X^q - X$, $Y^q - Y$, $A^q - A$, $B^q - B$ and $AX + B - Y$. The polynomial $AX + B - Y$ is not the characteristic polynomial F_V, but both F_V and $AX + B - Y$ have the same zeroes over $\mathbb{A}(4, \mathbf{F}_q)$. Therefore, Theorem 2.3.21 implies $I = \boldsymbol{I}(V)$. Let $\preceq_1$ denote the lexicographical order with $B > A > Y > X$. There are q^3 monomials not divisible by $LM_{\preceq_1}(X^q - X)$, $LM_{\preceq_1}(Y^q - Y)$, $LM_{\preceq_1}(A^q - A)$, $LM_{\preceq_1}(B^q - B)$ or $LM_{\preceq_1}(B + AX - Y)$ therefore $\{X^q - X, Y^q - Y, A^q - A, B^q - B, AX + B - Y\}$ is a Gröbner basis for $\boldsymbol{I}(V)$ under $\preceq_1$. It is easy to check that those polynomials are also a Gröbner basis under lexicographical order with $Y > X > A > B$.*

What about other Gröbner bases for $\boldsymbol{I}(V)$? Let $\preceq_2$ denote degree graded reverse lexicographical order with $X > Y > A > B$. The polynomials $X^q - X$, $Y^q - Y$, $A^q - A$, $B^q - B$ and $AX + B - Y$ are not a Gröbner basis for $\boldsymbol{I}(V)$ under $\preceq_2$. The polynomials

$$X^{q-i}(Y - B)^i - A^{i-1}(Y - B) \text{ and}$$

$$A^{q-i}(Y-B)^i - X^{i-1}(Y-B)$$

belong to $\boldsymbol{I}(V)$. *The monomials* X^iY^{q-i}, A^iY^{q-i}, AX *and* B^q *are leading monomials of elements of* $\boldsymbol{I}(V)$. *Therefore,* $X^q - X$, $Y^q - Y$, $A^q - A$, $B^q - B$, $AX + B - Y$, $X^{q-i}(Y-B)^i - A^{i-1}(Y-B)$ *and* $A^{q-i}(Y-B)^i - X^{i-1}(Y-B)$ *for* $i = 1, 2, \ldots q-1$ *are a Gröbner basis for* $\boldsymbol{I}(V)$ *under* $\preceq_2$. *Moreover they are also a Gröbner basis under degree graded reverse lexicographical order with* $A > B > X > Y$.

2.4 Affine Variety Codes

An affine variety code is a code generated by some polynomial functions over an affine variety. We have geometric information from the affine variety and algebraic information from the polynomial functions used for the code. Several good examples of affine variety codes are Reed–Solomon codes, cyclic codes and affine Grassmann codes.

Definition 2.4.1 *Let* $V := \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m\}$ *be an affine variety of* $\mathbb{A}(n, \mathbf{F}_q)$. *We define the evaluation map of* V *from* $\mathbf{F}_q[x_1, x_2, \ldots, x_n]$ *as:*

$$ev_V : \mathbf{F}_q[x_1, x_2, \ldots, x_n] \to \mathbf{F}_q^m$$

$$ev_V(f) \mapsto (f(\boldsymbol{p}_1), f(\boldsymbol{p}_2), \ldots, f(\boldsymbol{p}_m)).$$

We define the evaluation map of V *from* $\mathbf{F}_q[x_1, x_2, \ldots, x_n]/\boldsymbol{I}(V)$ *as:*

$$ev_V : \mathbf{F}_q[x_1, x_2, \ldots, x_n]/\boldsymbol{I}(V) \to \mathbf{F}_q^m$$
$$ev_V(f + \boldsymbol{I}(V)) \mapsto (f(\boldsymbol{p}_1), f(\boldsymbol{p}_2), \ldots, f(\boldsymbol{p}_m)).$$

By Theorem 2.3.14, the kernel of the map $ev_V : \mathbf{F}_q[x_1, x_2, \ldots, x_n] \to \mathbf{F}_q^m$ is $\mathbf{I}(V)$. The characteristic polynomial of $\mathbf{p}_i$, $F_{\mathbf{p}_i}$, evaluates to 1 at $\mathbf{p}_i$ and to 0 at all points of $V \setminus \mathbf{p}_i$. Therefore, the map ev_V is surjective. The first ring isomorphism theorem implies that $ev_V : \mathbf{F}_q[x_1, x_2, \ldots, x_n]/\mathbf{I}(V) \to \mathbf{F}_q^m$ is a well–defined isomorphism. We are abusing the notation ev_V because we are using it to define evaluation from two different rings. The definition is quite similar in both cases. For this reason, we will specify which definition is used.

Definition 2.4.2 *([FL98], Defn. 1.1) Suppose* $V := \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m\}$ *is an affine variety of* $\mathbb{A}(n, \mathbf{F}_q)$. *Let* $\bar{L}$ *be an* $\mathbf{F}_q$*-linear subspace of the quotient ring*

$\mathbf{F}_q[x_1, x_2, \ldots, x_n]/\boldsymbol{I}(V)$. *We define the* affine variety code of $\bar{L}$ evaluated at V *as*

$$C(V, \bar{L}) := \{ev_V(f) \mid f \in \bar{L}\}.$$

Definition 2.4.3 *([FL98], Defn. 1.1) Let* $V := \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m\}$ *be an affine variety of* $\mathbb{A}(n, \mathbf{F}_q)$. *Suppose* L *is an* $\mathbf{F}_q$*-linear subspace of* $\mathbf{F}_q[x_1, x_2, \ldots, x_n]$. *We define the* affine variety code of L evaluated at V *as*

$$C(V, L) := \{ev_V(f) \mid f \in L\}.$$

The length of $C(V, L)$ is $\#V$. Normally, the positions of a code C of length m are indexed by the integers $1, 2, \ldots, m$, but for an affine variety code $C(V, L)$ we may index the positions by V. If $\bar{L}$ is a subspace of $\mathbf{F}_q[x_1, x_2, \ldots, x_n]/\mathbf{I}(V)$, then the dimension of $C(V, \bar{L})$ is $\dim \bar{L}$. When L is a subspace of $\mathbf{F}_q[x_1, x_2, \ldots, x_n]$, then the dimension of $C(V, L)$ is $dim(L/(L \cap \mathbf{I}(V)))$.

Example 2.4.4 *The field* $\mathbf{F}_8$ *is equal to the ring* $\mathbf{F}_2[t]/\langle 1+t+t^3 \rangle$. *We consider the points of* $\mathbf{F}_8$ *as* $\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ *where* α *is a root of* $1 + t + t^3$. *The roots of* $1 + t + t^3$ *are* α, α^2 *and* α^4.

Consider $V := \{(x, y) \in \mathbf{F}_8^2 \mid 1+xy+(xy)^3 = 0\}$. *The set* V *is an affine variety of* $\mathbb{A}(2, \mathbf{F}_8)$. *We write* $V := \{(1, \alpha), (1, \alpha^2), (1, \alpha^4), (\alpha, 1), (\alpha, \alpha), \ldots, (\alpha^6, \alpha^5))\}$.

Let $L = Span_{\mathbf{F}_8}(\{1, Y, X, XY, X^3, X^3Y, Y^3, XY^3\})$. *If we evaluate the functions at each of the* 21 *points of* V *we obtain the following generator matrix for the code* $C(V, L)$.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\alpha & \alpha^2 & \alpha^4 & 1 & \alpha & \alpha^3 & \alpha^6 & 1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha & \alpha^4 & \alpha^5 & 1 & \alpha^3 & \alpha^4 & \alpha^6 & \alpha^2 & \alpha^3 & \alpha^5 \\
1 & 1 & 1 & \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^4 & \alpha^4 & \alpha^4 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^6 & \alpha^6 \\
\alpha & \alpha^2 & \alpha^4 & \alpha & \alpha^2 & \alpha^4 & \alpha & \alpha^2 & \alpha^4 & \alpha & \alpha^2 & \alpha^4 & \alpha & \alpha^2 & \alpha^4 & \alpha & \alpha^2 & \alpha^4 & \alpha & \alpha^2 & \alpha^4 \\
1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^5 & \alpha^5 & \alpha^5 & \alpha & \alpha & \alpha & \alpha^4 & \alpha^4 & \alpha^4 \\
\alpha & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^4 & \alpha^6 & \alpha^5 & \alpha^6 & \alpha & 1 & \alpha & \alpha^3 & \alpha^2 & \alpha^3 & \alpha^5 & \alpha^4 & \alpha^5 & 1 & \alpha^6 & 1 & \alpha^2 \\
\alpha^3 & \alpha^6 & \alpha^5 & 1 & \alpha^3 & \alpha^2 & \alpha^4 & 1 & \alpha^6 & \alpha & \alpha^4 & \alpha^3 & \alpha^5 & \alpha & 1 & \alpha^2 & \alpha^5 & \alpha^4 & \alpha^6 & \alpha^2 & \alpha \\
\alpha^3 & \alpha^6 & \alpha^5 & \alpha & \alpha^4 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha & \alpha^4 & 1 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^4 & 1 & \alpha^3 & \alpha^2 & \alpha^5 & \alpha & 1
\end{pmatrix}$$

The set $\{1, Y, X, XY, X^3, X^3Y, Y^3, XY^3\}$ *is a subset of the footprint of* $\boldsymbol{I}(V)$ *under degree graded reverse lexicographical order with* $X > Y$. *Therefore, the dimension of* $C(V, L)$ *is* 8. *We can use the footprint bound to prove the minimum distance of* $C(V, L)$ *is at least* 6. *We will later prove it is actually a* $[21, 8, 6]_{\mathbf{F}_8}$ *code.*

Usually affine variety codes are used to study codes from complicated algebraic objects. We present a few theorems on the intersection of two affine variety codes. The theorems will be useful to determine the dimension and a basis for graph based codes.

Theorem 2.4.5 *Let $V := \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m\}$ be an affine variety of $\mathbb{A}(n, \mathbf{F}_q)$. Let $\bar{L}$ and $\bar{M}$ be $\mathbf{F}_q$-linear subspaces of $\mathbf{F}_q[x_1, x_2, \ldots, x_n]/\boldsymbol{I}(V)$. Then*

$$C(V, \bar{L}) \cap C(V, \bar{M}) = C(V, \bar{L} \cap \bar{M}).$$

Proof.

As we remarked before, the map ev_V is an isomorphism between the linear spaces $\mathbf{F}_q[x_1, x_2, \ldots, x_n]/\mathbf{I}(V)$ and $\mathbf{F}_q^m$. The code $C(V, \bar{L})$ is simply the image of $\bar{L}$ under the map ev_V. The theorem states $ev_V(\bar{L}) \cap ev_V(\bar{M}) = ev_V(\bar{L} \cap \bar{M})$ which is a simple algebraic fact. □

Theorem 2.4.5 characterizes the intersection of two affine variety codes, provided the evaluation functions come from the quotient ring of the ideal. The next lemma states the intersection of the two affine variety codes when the evaluation functions are polynomials and not quotient ring elements. The lemma helps us compute the intersection of Theorem 2.4.5 in some cases. A preliminary version of this Lemma appears in [BHPJ13].

Lemma 2.4.6 *Let $V := \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m\}$ be an affine variety of $\mathbb{A}(n, \mathbf{F}_q)$. Let $\preceq_1$ and $\preceq_2$ be two monomial orders on $x_1, x_2, \ldots, x_n$. Let L be an $\mathbf{F}_q$-linear subspace of $Span_{\mathbf{F}_q}(\Delta_{\preceq_1}(\boldsymbol{I}(V)))$. In addition suppose that M is an $\mathbf{F}_q$-linear subspace of $Span_{\mathbf{F}_q}(\Delta_{\preceq_2}(\boldsymbol{I}(V)))$. Suppose $f_1, f_2, \ldots, f_s$ satisfy:*

$$Span_{\mathbf{F}_q}(\{f_1, f_2, \ldots, f_s\}) = \{f \in L \mid \exists g \in M \ : \ f - g \in \boldsymbol{I}(V)\}.$$

Then

$$C(V, L) \cap C(V, M) = C(V, Span_{\mathbf{F}_q}(\{f_1, f_2, \ldots, f_s\})).$$

Proof.

Suppose

$$c \in C(V, Span_{\mathbf{F}_q}(\{f_1, f_2, \ldots, f_s\})).$$

Then there exist $a_1, a_2, \ldots, a_s \in \mathbf{F}_q$ and f, such that

$$c = ev_V(f) \text{ and } f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s,$$

then

$$ev_V(f) \in C(V, L).$$

Note that

$$ev_V(f) = ev_V(f+h) \ \forall \ h \in \mathbf{I}(V).$$

Since

$$\exists g \in M \text{ such that } f - g \in \mathbf{I}(V),$$

then

$$ev_V(f) = ev_V(g + (f-g)) \in C(V, M).$$

Therefore,

$$C(V, Span_{\mathbf{F}_q}(\{f_1, f_2, \ldots, f_s\})) \subseteq C(V, L) \cap C(V, M).$$

For the reverse implication, let

$$\mathbf{c} \in C(V, L) \cap C(V, M).$$

There exist polynomials

$$f \in L \text{ and } g \in M, \text{ such that, } ev_V(f) = \mathbf{c} = ev_V(g).$$

This implies that

$$f - g \in (L + M) \cap \mathbf{I}(V).$$

Therefore,

$$f \in \{f \in L \mid \exists g \in M \ : \ f - g \in \mathbf{I}(V)\}.$$

From the conditions on $f_1, f_2, \ldots, f_s$ there exist $a_1, a_2, \ldots, a_s \in \mathbf{F}_q$, such that

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s,$$

which implies

$$\mathbf{c} \in C(V, Span_{\mathbf{F}_q}(\{f_1, f_2, \ldots, f_s\})).$$

□

The following corollary is useful to intersect two affine variety codes.

Corollary 2.4.7 *Let $V := \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m\}$ be an affine variety of $\mathbb{A}(n, \mathbf{F}_q)$. Let $\preceq_1$ and $\preceq_2$ be two monomial orders on $x_1, x_2, \ldots, x_n$. Let L be an $\mathbf{F}_q$-linear subspace of $Span_{\mathbf{F}_q}(\Delta_{\preceq_1}(\boldsymbol{I}(V)))$. In addition, suppose that M is an $\mathbf{F}_q$-linear subspace of $Span_{\mathbf{F}_q}(\Delta_{\preceq_2}(\boldsymbol{I}(V)))$. Then, the following are true:*

- *If $h \in \{f \in L \mid \exists g \in M \ : \ f - g \in \boldsymbol{I}(V)\}$, then $h - rem_{\preceq_2}(h)$ belongs to $(L + M) \cap \boldsymbol{I}(V)$.*
- *If $h \in (L+M) \cap \boldsymbol{I}(V)$, then $\exists \ f \in \{f \in L \mid \exists g \in M \ : \ f - g \in \boldsymbol{I}(V)\}$ such that $h = f - rem_{\preceq_2}(f)$.*

PROOF.

We begin with the first statement. Let $h \in L$. We know $rem_{\preceq_2}(h)$ is the unique polynomial in $Span_{\mathbf{F}_q}(\Delta_{\preceq_2}(\mathbf{I}(V)))$, such that $h - rem_{\preceq_2}(h)$ is an element of $\mathbf{I}(V)$. If $h \in \{f \in L \mid \exists g \in M \ : \ f - g \in \mathbf{I}(V)\}$, then there exists a $g \in M \subseteq Span_{\mathbf{F}_q}(\Delta_{\preceq_2}(\mathbf{I}(V)))$, such that $h - g \in \mathbf{I}(V)$. Thus, g must equal $rem_{\preceq_2}(h)$ and, therefore, $h - rem_{\preceq_2}(h) = h - g \in (L+M) \cap \mathbf{I}(V)$. This finishes the proof of the first statement. Now let $h \in (L+M) \cap \mathbf{I}(V)$, i.e., $h = f - g$, where $g \in M$ and $f \in L$. By the definition of the remainder we know $g - rem_{\preceq_2}(f)$. Therefore, f is the polynomial $f \in \{f \in L \mid \exists g \in M \ : \ f - g \in \mathbf{I}(V)\}$ such that $h = f - rem_{\preceq_2}(f)$. □

We can also use the footprint bound to get a bound on the minimum distance of the code. For an affine variety code $C(V, L)$, a polynomial $f \in L$ and $\langle g_1, g_2, \ldots, g_s \rangle = \mathbf{I}(V)$ we give an upper bound on the number of zeroes of f in V, which gives a lower bound on the weight of the codeword $ev_V(f)$. A Gröbner basis for $\langle g_1, g_2, \ldots, g_s, f \rangle$, then Theorem 2.3.16 gives the exact number of zeroes of f. However, finding a Gröbner basis for each ideal of the form $\{g_1, g_2, \ldots, g_s, f\}$ usually is quite difficult, so we may settle for the upper bound given in Theorem 2.3.17.

The authors of [FL98] remark that any code is an affine variety code. The key aspect is to find affine varieties suited to constructing codes. There are many codes constructed in this way and we give some examples now.

2.4.1 Reed–Solomon codes

Reed–Solomon codes are among the most prominent codes in algebraic coding theory. We define them as follows:

DEFINITION 2.4.8 *Consider the univariate polynomial ring* $\mathbf{k}[t]$. *We denote the* $\mathbf{F}_q$*–vector subspace generated by* $1, t, t^2, \ldots, t^{k-1}$ *by* $\mathbf{k}[t]_{<k}$.

DEFINITION 2.4.9 *([Lin91]) Let* $\emptyset \neq V \subseteq \mathbb{A}(1, \mathbf{F}_q)$. *The* Reed–Solomon code of dimension k over V *is defined as*

$$RS(V, k) := C(V, \mathbf{k}[t]_{<k}).$$

As we may expect, the length of the Reed–Solomon codes depends on the number of elements of $\mathbf{F}_q$ we pick as our evaluation points. If $1 \leq k \leq \#V$, then

the monomials $1, t, t^2, \ldots, t^{k-1}$ are equal to their remainders when divided by $\Pi_{\alpha \in V}(t - \alpha)$. We can use the footprint bound (or the fundamental theorem of algebra) to say a nonzero codeword of $RS(V, k)$ has at most $k - 1$ zeroes. Therefore, Reed-Solomon codes are MDS codes. Please note that the positions of $RS(V, k)$ are indexed by the integers $1, 2, \ldots, \#V$ or by the elements of V. Indexing the code positions by the affine variety points brings the code closer to its algebraic roots. This will be useful later on.

2.4.2 Cyclic codes

Definition 2.4.10 *Let $S \subseteq \mathbb{Z}_{q-1}$. We denote the $\mathbf{F}_q$–vector subspace of $\mathbf{k}[t]_{<q}$ generated by $\{t^i \mid i \in S\}$ by $\mathcal{M}_t(S)$.*

Definition 2.4.11 *Let $S \subseteq \mathbb{Z}_{q-1}$. The code $C(\mathbf{F}_q^*, \mathcal{M}_t(S))$ is a* cyclic code.

For any codeword $\mathbf{c} = (f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) \in C(\mathbf{F}_q^*, \mathcal{M}_t(S))$ the cyclic shift of $\mathbf{c}$, i.e. $(f(\alpha), f(\alpha^2), f(\alpha^3), \ldots, f(1))$, is also in $C(\mathbf{F}_q^*, \mathcal{M}_t(S))$. The Reed–Solomon codes $RS(\mathbf{F}_q^*, k)$ are also cyclic codes with $S = \{0, 1, \ldots, k-1\}$. When S is the shift of k consecutive integers, (i.e. $S = \{i, i+1, \ldots, i+k-1\}$) then $C(\mathbf{F}_q^*, \mathcal{M}_t(S))$ is monomially equivalent to a Reed–Solomon code.

2.4.3 Affine Grassmann codes

These codes were introduced in in [HBG10]. The same authors studied their duals as affine variety codes in [BGH12].

Definition 2.4.12 *Let $\boldsymbol{M}$ be an $\ell \times \ell'$ matrix, where $\ell \leq \ell'$. Suppose I is a subset of $\{1, 2, \ldots, \ell\}$ and $J \subseteq \{1, 2, \ldots, \ell'\}$. Suppose $\#I = \#J = h \leq r$. Let $M_{I,J}$ denote the submatrix of M obtained from the rows specified by I and the columns specified by J. An h-minor of $\boldsymbol{M}$ is the determinant of an $h \times h$ submatrix of $\boldsymbol{M}$. The minor determined by I and J is denoted by $det(\boldsymbol{M}_{I,J})$.*

Consider the set of $\ell \times \ell'$ matrices over $\mathbf{F}_q$, $\mathbb{M}^{\ell \times \ell'}(\mathbf{F}_q)$. We identify $\mathbb{M}^{\ell \times \ell'}(\mathbf{F}_q)$ with the points of $\mathbb{A}(\ell\ell', \mathbf{F}_q)$. We associate to this affine space the polynomial ring $\mathbf{F}_q[\mathbf{X}]$. The polynomial ring is defined in the $\ell\ell'$ indeterminate entries of $\mathbf{X} := (X_{i,j})_{1 \leq i \leq \ell, 1 \leq j \leq \ell'}$. We denote $\sigma_h(\mathbf{X})$ as the set of all h-minors of $\mathbf{X}$.

Definition 2.4.13 *We define the* affine Grassmann code, *$\mathcal{C}^{\mathbb{A}}(\ell, \ell + \ell')$, as the affine variety code $C(\mathbf{F}_q[\boldsymbol{X}], Span_{\mathbf{F}_q}(\sigma_0(\boldsymbol{X}) \cup \sigma_1(\boldsymbol{X}) \cup \ldots \cup \sigma_h(\boldsymbol{X})))$.*

Chapter 3

Graph Based Codes

In this chapter, we introduce two classes of graph based codes: Tanner codes and graph codes. Tanner codes, also known as generalized LDPC codes, are a class of codes built from a graph and a smaller component code. Several different codes may be constructed from the same graph and component code, but we can always gleam some information. For example, there are iterative decoding algorithms, and bounds on the parameters of the codes. We start with some basic definitions from Graph Theory.

3.1 Bipartite Graphs

Definition 3.1.1 *A bipartite graph G is a triple $(V_1(G), V_2(G), E(G))$ where $V_1(G)$ and $V_2(G)$ are finite sets and $E(G) \subseteq V_1(G) \times V_2(G)$. The elements of $V_1(G)$ and $V_2(G)$ are called* vertices *(sing. vertex). Two vertices v and u are* adjacent*, if and only if $(v, u) \in E(G)$. We say either v or u are* incident *to the edge (v, u). The vertices v and u are the* endpoints *of the edge (v, u).*

Definition 3.1.2 *Let G be a bipartite graph. For a vertex $v \in V_1(G)$, we define the* neighborhood *of v as $\{u \in V_2(G) \mid (v, u) \in E(G)\}$. For a vertex $u \in V_2(G)$, we define the* neighborhood *of u as $\{v \in V_1(G) \mid (v, u) \in E(G)\}$.*

The neighborhood of a vertex u is denoted by $\mathcal{N}(u)$. For a vertex v, we denote the set of edges incident to v by $E(v)$.

Note that for any vertex $v \in V_1(G)$ a vertex $u \in \mathcal{N}(v)$, if and only if $(v,u) \in E(v)$. For any $u \in V_2(G)$, there is a similar correspondence between $\mathcal{N}(u)$ and $E(u)$.

In order to simplify the graph based code construction, we impose a regularity condition. We define regularity as follows.

Definition 3.1.3 *Let G be a bipartite graph. If $\forall\ v \in V_1(G)\ :\ \#\mathcal{N}(v) = n_1$ and $\forall\ u \in V_2(G)\ :\ \#\mathcal{N}(u) = n_2$ then G is a* (n_1, n_2)-regular bipartite graph. *We also denote $\#V_1(G)$ by m_1 and $\#V_2(G)$ by m_2.*

Note that a (n_1, n_2)-regular bipartite graph has $m_1 n_1 = m_2 n_2$ edges.

3.2 Graph Based Codes

Definition 3.2.1 *Let G be a (n_1, n_2)-regular bipartite graph. Let S_1 be a set of cardinality n_1 and S_2 a set of cardinality n_2. Typically, $S_1 = \{1, 2, \ldots, n_1\}$ and $S_2 = \{1, 2, \ldots, n_2\}$, but sometimes another choice is suitable. Suppose that for each $v \in V_1(G)$, χ_v is a bijection from S_1 to $E(v)$ and for each $u \in V_2(G)$, ϕ_u is a bijection from S_2 to $E(u)$. The bipartite graph G with the bijections described for each vertex is called an* endpoint labeled graph.

Please note that ϕ_u induces a bijection $\gamma_u : S_2 \to \mathcal{N}(u)$ by $\phi_u(i) = (\gamma_u(i), u)$. We define the two classes of graph based codes now.

Definition 3.2.2 *[Tan81]*

Suppose G is an (n_1, n_2)-regular endpoint labeled bipartite graph. For a vertex $u \in V_2(G)$, we define

$$\boldsymbol{c}_{\mathcal{N}(u)} := (c_{\gamma_u(1)}, c_{\gamma_u(2)}, \ldots, c_{\gamma_u(n_2)}) \in \mathbf{F}_q^{n_2}.$$

Let C be a code of length n_2 over $\mathbf{F}_q$. We define the Tanner code

$$(G, C) := \{(c_u) \in \mathbf{F}_q^{m_1} \mid \forall\ u \in V_2(G) :\ \boldsymbol{c}_{\mathcal{N}(u)} \in C\}.$$

The code (G, C) is a code of length m_1. We may identify the positions of the Tanner code (G, C) with the integers $1, 2, \ldots, m_1$ as is normally done in coding theory. We prefer to identify the positions of (G, C) with the vertices of $V_1(G)$ since the vertices of $V_1(G)$ contain the symbols of the codewords. The vertices of $V_1(G)$ are also known as the *variable nodes*. The vertices of $V_2(G)$ are called the *constraint nodes* because they represent the parity check equations (G, C) must satisfy.

We may also define Tanner codes in terms of projections. The Tanner code (G, C) is a code, such that for any vertex $u \in V_2(G)$ the code $(G, C)^{\mathcal{N}(u)}$ is contained in a monomially equivalent code to C. This is the key concept behind the Tanner code. A Tanner code is a long code, which is built from several copies of the shorter component code. The copies are joined together according to the graph G. This definition is closer to Tanner's own definition in [Tan81], but our definition makes the code construction absolutely precise.

Definition 3.2.3 *[Tan81, Rot06]*

Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph. For

$$\boldsymbol{c} = (c_{(v,u)})_{(v,u)\in E(G)} \in \mathbf{F}_q^{\#E(G)},$$

and a vertex $u \in V_2(G)$, we define the subvector

$$\boldsymbol{c}_{E(u)} := (c_{\phi_u(1)}, c_{\phi_u(2)}, \ldots, c_{\phi_u(n_2)}) \in \mathbf{F}_q^{n_2}.$$

Likewise, for the same vector $\boldsymbol{c}$ and a vertex $v \in V_1(G)$, we define the subvector

$$\boldsymbol{c}_{E(v)} := (c_{\chi_v(1)}, c_{\chi_v(2)}, \ldots, c_{\chi_v(n_1)}) \in \mathbf{F}_q^{n_1}.$$

Let C_1 be a code of length n_1 over $\mathbf{F}_q$ and let C_2 be a code of length n_2 over $\mathbf{F}_q$.

We define the following codes:

- *The left auxiliary graph code:*

$$(G, C_1 : \mathbf{F}_q^{n_2}) := \{(c_{(v,u)}) \in \mathbf{F}_q^{\#E(G)} \mid \forall\ v \in V_1(G) :\ \boldsymbol{c}_{E(v)} \in C_1\},$$

- *The right auxiliary graph code:*

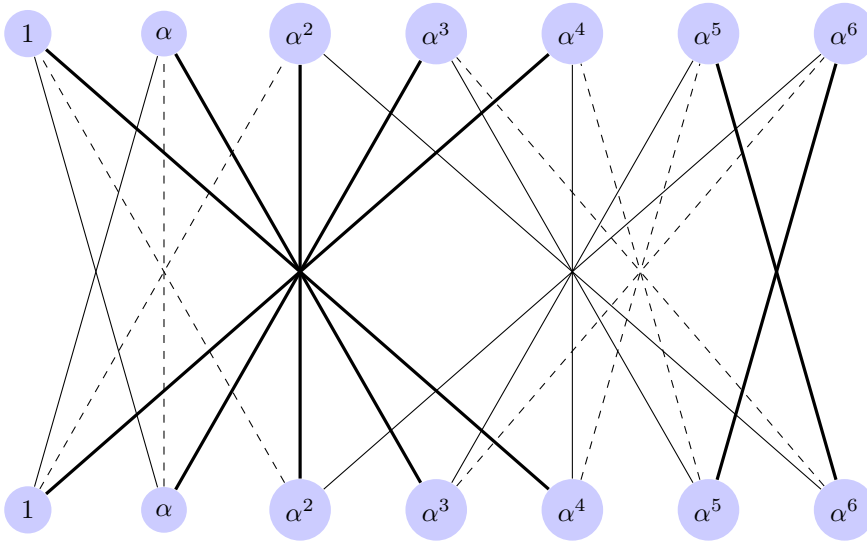
$$(G, \mathbf{F}_q^{n_1} : C_2) := \{(c_{(v,u)}) \in \mathbf{F}_q^{\#E(G)} \mid \forall\ u \in V_2(G) :\ \boldsymbol{c}_{E(u)} \in C_2\},$$

- *The Graph code:*

$$(G, C_1 : C_2) := (G, C_1 : \mathbf{F}_q^{n_2}) \cap (G, \mathbf{F}_q^{n_1} : C_2).$$

A graph code, like Tanner codes, could also be defined in terms of projections. The graph code $(G, C_1 : C_2)$ is a code where $(G, C_1 : C_2)^{E(v)}$ is contained in a code monomially equivalent to C_1, and $(G, C_1 : C_2)^{E(u)}$ is contained in a monomially equivalent code to C_2.

Example 3.2.4 *Let G be the following $(3,3)$-regular endpoint labeled bipartite graph:*



Note that $V_1(G) = V_2(G) = \mathbf{F}_8^*$. Let $V := V(1 + t + t^3) = \{\alpha, \alpha^2, \alpha^4\}$ be an affine variety of $\mathbb{A}(1, \mathbf{F}_8)$. The edge set $E(G) := \{(x, y) \in \mathbf{F}_8^* \times \mathbf{F}_8^* \mid xy \in V\}$. The edge labelings are as follows:

$$\text{For } x \in V_1(G) \ : \ \phi_x : V \to E(x)$$

$$\phi_x(v_i) := (x, \frac{v_i}{x})$$

$$\text{For } x \in V_2(G) \ : \ \chi_y : V \to E(y)$$

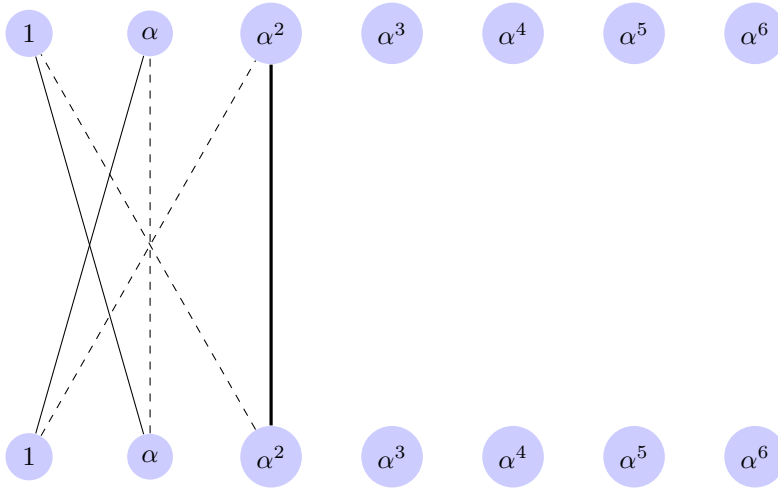
$$\chi_y(v_i) := (\frac{v_i}{y}, y).$$

Note that the drawing style of the edge (x, y) depends of the value of xy. If $xy = \alpha$, then the edge is a solid line, if $xy = \alpha^2$, then the line is a dashed line and otherwise, the edge is a thick line. We would like to determine the graph code $(G, RS(V, 2) : RS(V, 2))$. Since $RS(V, 2)$ is a $[3, 2, 2]$ code, the value of any two coordinates determines the third coordinate.

The Reed–Solomon code $RS(V, 2)$ has the following generator matrix:

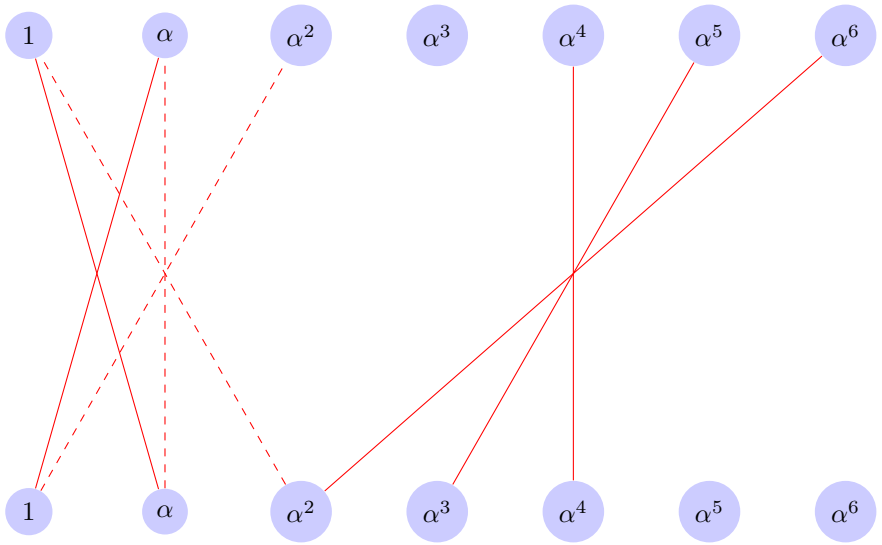
$$\begin{pmatrix} 1 & 0 & \alpha^5 \\ 0 & 1 & \alpha^4 \end{pmatrix}.$$

Another codeword of weight 2 is $(1, \alpha, 0)$. The first column corresponds to α, the second column corresponds to α^2 and the third column corresponds to α^4. If we encode 1 at the two thin edges, α at the three dashed edges and α^5 at the thick edge, we can encode the rest of the edges with zeroes.

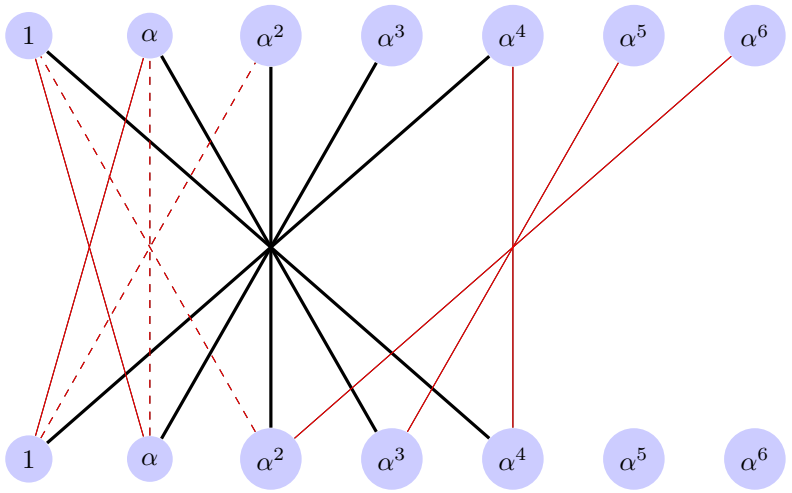


Note that around each vertex, the symbols assigned to the edges are codewords of $RS(V, 2)$. We have found a codeword of the graph code $(G, RS(V, 2) : RS(V, 2))$.

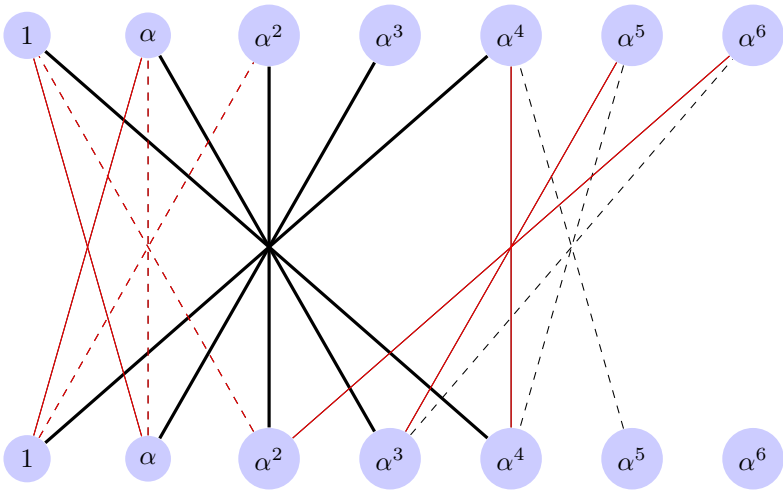
With the rule that the value of any two edges incident to a vertex determines the value of the third edge incident to the same vertex we show that a codeword of $(G, RS(V, 2) : RS(V, 2))$ is determined by the $\mathbf{F}_8$ symbols at the following edges:



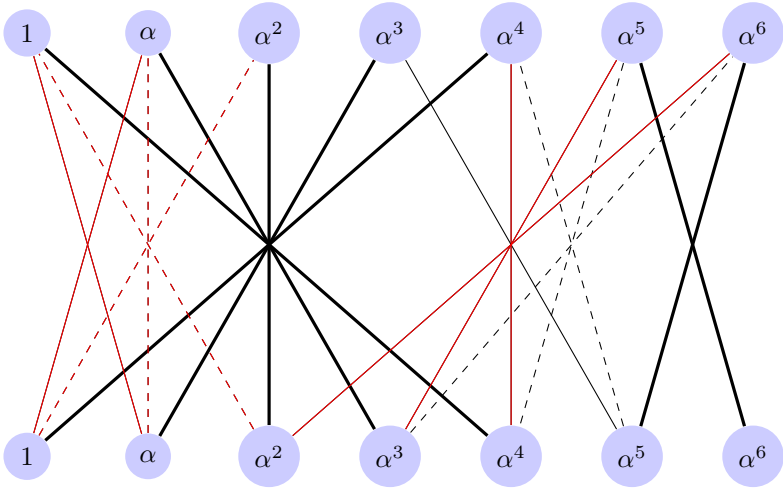
We suppose the $\mathbf{F}_8$ *symbols at each of the* 8 *edges have been determined. Now the following edges have also been determined from the conditions given by* $RS(V, 2)$*:*



Now that these edges have been determined, they also determine the $\mathbf{F}_8$ *symbols of these additional edges:*



Now the following edges are also determined:



Clearly, the $\mathbf{F}_8$ *symbols at all edges are determined from the first* 8 *edges. It is not clear that these* 8 *positions are information positions for the graph code* $(G, RS(V,2) : RS(V,2))$*. In fact, it may happen that we could assign symbols to the* 8 *edges such that there is no codeword with those values at those positions. However, we now prove the dimension of* $(G, RS(V,2) : RS(V,2))$ *is* 8*.*

Suppose f *is an* $\mathbf{F}_8$*-linear combination of* $1, Y, X, XY, X^3, X^3Y, Y^3, XY^3$*. We may consider* $f(X,Y)$ *as a function on the edge set. At the vertex* $x \in V_1(G)$*,* f *takes on the values* $f(x,Y)$*. The edges incident to* x *satisfy* $1 + xY + (xY)^3 = 0$*,*

therefore $f(x, Y)$ is a linear combination of 1 and Y. In conclusion, the graph code $(G, RS(V,2) : RS(V,2))$ is the code from Example 2.4.4. Since we know the minimum distance is at least 6, and we have found a codeword of weight 6, the graph code $(G, RS(V,2) : RS(V,2))$ is a $[21, 8, 6]_{\mathbf{F}_8}$ code.

The notation we have chosen for graph codes and Tanner codes follows closely the notation from [Rot06]. Now we present another relation between Tanner codes and graph codes.

Theorem 3.2.5 *[Tan81] Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph and C be an $[n_2, k_2, d_2]$ code. Suppose C_1 is the $[n_1, 1, n_1]$ repetition code. Then, the code $(G, C_1 : C)$ is an n_1-fold repetition code of (G, C).*

Proof.

Consider the map $\tau : \mathbf{F}_q^{V_1(G)} \to \mathbf{F}_q^{E(G)}$, if $\tau(\mathbf{x}) = \mathbf{y}$, then $y_e := x_u$ where $u \in V_1(G)$ is incident to edge e. Note that $\tau((G, \mathbf{F}_q^{n_2})) = (G, C_1 : \mathbf{F}_q^{n_2})$. Suppose $\tau(\mathbf{x}) = \mathbf{y}$. For any $v \in V_1(G)$ the subvector $\mathbf{y}_{E(v)} = (y_{\phi_v(1)}, y_{\phi_v(2)}, \ldots, y_{\phi_v(n_2)})$ is equal to $\mathbf{x}_{\mathcal{N}(v)} = (x_{\gamma_u(1)}, x_{\gamma_u(2)}, \ldots, x_{\gamma_u(n_2)})$. Therefore, $\mathbf{x} \in (G, C)$ if and only if $\mathbf{y} \in (G, C_1 : C)$. □

Tanner presented these two closely related constructions of graph based codes in [Tan81]. In his article, Tanner gave examples of cases where the graph code properties depend on the labeling functions ϕ_v. Nonetheless, he gave bounds on the code parameters independent of any labelings. Now we present Tanner's dimension bounds.

Theorem 3.2.6 *[Tan81] Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph. Let C be an $[n_2, k_2, d_2]$ code. Then, the dimension of (G, C) is at least*

$$m_1 - m_2(n_2 - k_2).$$

Tanner simply counts the parity check equations of the code. There are $n_2 - k_2$ parity check equations for each of the m_2 check nodes of $V_2(G)$. Therefore the codimension of the code is at most $m_2(n_2 - k_2)$. With the same technique Tanner bounds the dimension of graph codes.

Theorem 3.2.7 *[Tan81] Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph. Let C_1 be an $[n_1, k_1, d_1]$ code and let C_2 be an $[n_2, k_2, d_2]$ code. Then, the dimension of the graph code $(G, C_1 : C_2)$ is at least*

$$\#E(G) - m_1(n_1 - k_1) - m_2(n_2 - k_2)$$

Tanner's proof is to overestimate the number of parity check equations of the graph code with the parity checks equations of the auxiliary graph codes. In fact, we will soon prove that this bound is sharp for the auxiliary graph codes. It turns out that the auxiliary graph codes are very useful in understanding graph codes. The next theorem states the structure of the auxiliary graph codes explicitly.

Lemma 3.2.8 *Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph. Let C_1 be an $[n_1, k_1, d_1]$ code and let C_2 be an $[n_2, k_2, d_2]$ code. Then,*

- $(G, \mathbf{F}_q^{n_1} : C_2) \equiv C_2 \times C_2 \times \cdots \times C_2 \subseteq \mathbf{F}_q^{m_2 n_2}$,
- $(G, C_1 : \mathbf{F}_q^{n_2}) \equiv C_1 \times C_1 \times \cdots \times C_1 \subseteq \mathbf{F}_q^{m_1 n_1}$.

Proof.

Let ϕ_u be the labeling for $u \in V_1(G)$ for $(G, C_1 : \mathbf{F}_q^{n_2})$. Suppose $V_1(G)$ is the set $\{1, \ldots, m_1\}$. The labelings ϕ_u for $u \in V_1(G)$ induce a bijection ϕ from the set $\{1, 2, \ldots, m_1 n_1\}$ to $E(G)$ as follows: $\phi(n_1(i-1)+j) := (i, \phi_i(j))$. Suppose $\mathbf{c} \in (G, C_1 : \mathbf{F}_q^{n_2})$. Let $c_u := \mathbf{c}_{E(u)}$. The map ϕ sends $\mathbf{c}$ to $(c_1, c_2, \ldots, c_{m_1})$. This establishes the equivalence between $(G, C_1 : \mathbf{F}_q^{n_2})$ and $C_1 \times C_1 \times \cdots \times C_1$. □

Lemma 3.2.9 *Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph. Let C_1 be an $[n_1, k_1, d_1]$ code and let C_2 be an $[n_2, k_2, d_2]$ code. Then,*

- $(G, \mathbf{F}_q^{n_1} : C_2^{\perp}) = (G, \mathbf{F}_q^{n_1} : C_2)^{\perp}$,
- $(G, C_1^{\perp} : \mathbf{F}_q^{n_2}) = (G, C_1 : \mathbf{F}_q^{n_2})^{\perp}$.

Proof.

We denote the code $C_1 \times C_1 \times \cdots \times C_1 \subseteq \mathbf{F}_q^{m_1 n_1}$ as $\prod_{i=1}^{m_1} C_1$. Likewise, we denote $C_1^{\perp} \times C_1^{\perp} \times \cdots \times C_1^{\perp} \subseteq \mathbf{F}_q^{m_1 n_1}$ as $\prod_{i=1}^{m_1} (C_1^{\perp})$. Note that clearly $(\prod_{i=1}^{m_1} C_1)^{\perp} = (\prod_{i=1}^{m_1} C_1^{\perp})$ By hypothesis, $(G, C_1 : \mathbf{F}_q^{n_2})$ and $(G, C_1^{\perp} : \mathbf{F}_q^{n_2})$ are constructed with the same (n_1, n_2)-regular bipartite labeled graph. From Lemma 3.2.8, there is a bijection $\phi : \{1, 2, \ldots, m_1 n_1\} \to E(G)$, such that $\phi(\prod_{i=1}^{m_1} C_1) = (G, C_1 : \mathbf{F}_q^{n_2})$ and

$\phi(\prod_{i=1}^{m_1}(C_1^{\perp})) = (G, C_1^{\perp} : \mathbf{F}_q^{n_2})$. Since $\phi(\prod_{i=1}^{m_1}(C_1^{\perp})) = \phi(\prod_{i=1}^{m_1}(C_1)^{\perp}) = \phi(\prod_{i=1}^{m_1}(C_1))^{\perp}$, we obtain that the dual code of $(G, C_1^{\perp} : \mathbf{F}_q^{n_2})$ is actually $(G, C_1 : \mathbf{F}_q^{n_2})$. The other case is similar. □

Theorem 3.2.10 *Suppose G is an (n_1, n_2)-regular bipartite endpoint labeled graph. Let C_1 be an $[n_1, k_1, d_1]$ code and let C_2 be an $[n_2, k_2, d_2]$ code. Then,*

$$(G, C_1 : C_2)^{\perp} = (G, C_1^{\perp} : \mathbf{F}_q^{n_2}) + (G, \mathbf{F}_q^{n_1} : C_2^{\perp}).$$

Proof.

From [MS77] we have the following equality for any two vector spaces codes C and D;

$$(C \cap D)^{\perp} = C^{\perp} + D^{\perp}.$$

We use this equality to prove the last part. From the definition of a graph code,

$$(G, C_1 : C_2) = (G, \mathbf{F}_q^{n_1} : C_2) \cap (G, C_1 : \mathbf{F}_q^{n_2}).$$

This implies their dual codes are equal, that is

$$(G, C_1 : C_2)^{\perp} = ((G, \mathbf{F}_q^{n_1} : C_2) \cap (G, C_1 : \mathbf{F}_q^{n_2}))^{\perp}.$$

Now we apply $(C \cap D)^{\perp} = C^{\perp} + D^{\perp}$ to obtain

$$(G, C_1 : C_2)^{\perp} = (G, \mathbf{F}_q^{n_1} : C_2)^{\perp} + (G, C_1 : \mathbf{F}_q^{n_2})^{\perp}.$$

Lemma 3.2.9 implies that we may rewrite the right hand side with auxiliary graph codes with $C_1^{\perp}$ and $C_2^{\perp}$ as component codes. We obtain

$$(G, C_1 : C_2)^{\perp} = (G, \mathbf{F}_q^{n_1} : C_2^{\perp}) + (G, C_1^{\perp} : \mathbf{F}_q^{n_2}).$$

□

With these key observations we can find the check equations which both codes have in common.

Corollary 3.2.11 *Let G be an (n_1, n_2)-regular bipartite labeled graph. Let C_1 be an $[n_1, k_1, d_1]$ code and let C_2 be an $[n_2, k_2, d_2]$ code. Then*

$$\#E(G) - \dim(G, C_1 : C_2) = m_1(n_1 - k_1) + m_2(n_2 - k_2) - \dim(G, C_1^{\perp} : C_2^{\perp}).$$

PROOF.

By Theorem 3.2.10 $(G, C_1 : C_2)^\perp$ is $(G, C_1^\perp : \mathbf{F}_q^{n_2}) + (G, \mathbf{F}_q^{n_1} : C_2^\perp)$. The vector space $(G, C_1^\perp : \mathbf{F}_q^{n_2})$ is the space of parity checks from the vertices in $V_1(G)$. It has dimension $m_1(n_1 - k_1)$. The space $(G, \mathbf{F}_q^{n_1} : C_2^\perp)$ is the space of parity checks from $V_2(G)$. This space has dimension $m_2(n_2 - k_2)$. The set of common parity checks is $(G, C_1^\perp : \mathbf{F}_q^{n_2}) \cap (G, \mathbf{F}_q^{n_1} : C_2^\perp)$ but that is the definition of the graph code $(G, C_1^\perp : C_2^\perp)$ and the theorem follows. □

We point out the following peculiarity from the dimension formula in Corollary 3.2.11: if $\#E(G) = m_1(n_1 - k_1) + m_2(n_2 - k_2)$, as it happens for a (n_1, n_1) regular graph with $k_2 = n_1 - k_1$, then $\dim(G, C_1 : C_2) = \dim(G, C_1^\perp : C_2^\perp)$. Therefore the orthogonal codes $(G, C_1 : C_2)$ and $(G, C_1^\perp : C_2^\perp)$ have the same dimension.

3.3 Examples

As Tanner remarked himself, any code can be realized as a Tanner code. We give some significant examples of Tanner and graph codes.

DEFINITION 3.3.1 *Let $G = (V_1(G), V_2(G), E(G))$ be a bipartite graph. If $E(G) = V_1(G) \times V_2(G)$, then G is the* complete bipartite graph on m_1 and m_2 vertices. *We denote G by K_{m_1,m_2}.*

Note that for any $v \in V_1(K_{m_1,m_2})$ the equality $\mathcal{N}(v) = V_2(K_{m_1,m_2})$ holds. Likewise for any $u \in V_2(K_{m_1,m_2})$ we have that $\mathcal{N}(u) = V_1(K_{m_1,m_2})$. The graph K_{m_1,m_2} is a (m_2, m_1)-regular bipartite graph.

EXAMPLE 3.3.2 (A CODE C) *Let C be a $[n, k, d]$ code. Let $V_1(K_{n,1})$ be the set of positions of the code C. Suppose $V_2(K_{n,1}) = \{u\}$. The vertex labeling $\phi_u : \{1, 2, \ldots, n\} \to V_1(K_{n,1})$ is the identity. Then, C equals $(K_{n,1}, C)$.*

EXAMPLE 3.3.3 (PRODUCT CODES [TAN81]) *Suppose C_1 and C_2 are an $[n_1, k_1, d_1]$ code and an $[n_2, k_2, d_2]$ code respectively. We construct K_{n_2,n_1} such that $V_1(K_{n_2,n_1})$ is the set of positions of C_2 and $V_2(K_{n_2,n_1})$ is the set of positions of C_1. For $v \in V_1(K_{n_2,n_1})$ the bijection $\chi_v : \{1, 2, \ldots, n_1\} \mapsto E(v)$ is defined as $\chi_v(i) := (v, i)$. Likewise for $u \in V_2(K_{n_2,n_1})$ the edge labeling $\phi_u : \{1, 2, \ldots, n_2\} \mapsto E(u)$ is defined as $\phi_u(i) := (i, u)$. The graph code $(K_{n_2,n_1}, C_1 : C_2)$ is the product code of C_1 and C_2.*

Tanner [Tan81] already shows the importance of the labelings for graph based codes. Taking the graphs $G = K_{7,7}$ and the $[7, 4, 3]$ Hamming code as component codes, he gives three graph codes with completely different parameters: the $[49, 16, 9]$ product code, a $[49, 12, 16]$ code and a $[49, 7, 17]$ code.

Example 3.3.4 (Code of a bipartite graph) *Let G be an (n_1, n_2) regular bipartite graph. Let M be a $V_1(G) \times V_2(G)$ matrix whose entries are 0 and 1. Suppose that the entry $M_{i,j} = 1$ if and only if $(i, j) \in E(G)$. The code of G is defined as the dual code of the rowspace of M. We denote it by $C(G)$. For any labeling, the code $C(G)$ is equal to the Tanner code (G, C_2), where C_2 is the $[n_1, n_1 - 1, 2]$ zero sum code. Several codes which fall under this example are Reed–Muller codes, codes of finite geometries, designs and incidence structures, LDPC codes and cyclic codes to name a few.*

We can also use a code to get a graph as follows.

Definition 3.3.5 *[Tan81]*

Let C be a binary code of length n. Suppose $C^\perp$ is generated by its codewords of weight d_1. The Tanner graph of C *is the following graph. The vertex set $V_1(G(C)) := \{1, 2, \ldots, n\}$. We identify this vertex set with the set of positions of C. The vertex set $V_2(G(C)) := \{\boldsymbol{c} \in C^\perp \mid wt(\boldsymbol{c}) = d_1\}$. We identify this vertex set with the set of codewords of $C^\perp$ of weight d_1. The edge set is given by $E(G(C))) := \{(i, \boldsymbol{c}) \in V_1(G(C)) \times V_2(G(C))) \mid c_i \neq 0\}$.*

Since $C^\perp$ is a binary code generated by its codewords of weight d_1, then the code of the Tanner graph $C(G(C))$ is C itself. The code C is also equal to the Tanner code $(G(G), [d_1, d_1 - 1, 2]_{\mathbf{F}_2})$. One also may study G by considering $C(G)$ over other prime fields by taking the component code to be $[d_1, d_1 - 1, 2]_{\mathbf{F}_p}$.

Chapter 4

Graph Codes with Cyclic Component Codes

The subfield subcode technique is designed to obtain codes over a small, simple alphabet. Now we apply this technique to some interesting graph codes with cyclic component codes. Some of these Tanner codes turned out to be optimal. This finding is published in [HPZ14].

First, we introduce the notion of subfield subcodes. Then, we introduce the Tanner codes. We finish this chapter discussing some of the optimal codes we found with this construction and other interesting results.

4.1 Subfield Subcodes

Several codes are constructed as subfield subcodes. For example, BCH codes are subfield subcodes of Reed–Solomon codes. The material in this section follows [Sti90]. We begin by giving some preliminary concepts related to fields.

The trace function from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ is $tr : x \mapsto x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$. The trace function is a $\mathbf{F}_q$-linear epimorphism from the additive group of $\mathbf{F}_{q^m}$ to the additive group of $\mathbf{F}_q$.

Definition 4.1.1 *Let $\boldsymbol{x} \in \mathbf{F}_{q^m}^n$. Suppose C is a code over $\mathbf{F}_{q^m}$ of length n. We define the following:*

- $\boldsymbol{x}^{(q)} := (x_1^q, x_2^q, \ldots, x_n^q) \in \mathbf{F}_{q^m}^n$,
- $C^{(q)} := \{\boldsymbol{c}^{(q)} \mid \boldsymbol{c} \in C\}$,
- *The* subfield subcode *of C, denoted by $C|\mathbf{F}_q$, is defined as $C \cap \mathbf{F}_q^n$,*
- $tr(\boldsymbol{x}) := (tr(x_1), tr(x_2), \ldots, tr(x_n)) \in \mathbf{F}_q^n$,
- *The* trace code *of C, denoted by $tr(C)$ is defined as $\{tr(\boldsymbol{c}) \mid \boldsymbol{c} \in C\}$,*
- *C is* q-invariant *if $C = C^{(q)}$.*

Since we are working over $\mathbf{F}_{q^m}$ the code $C^{(q)}$ is also an $\mathbf{F}_{q^m}$-linear code. Note that both the subfield subcode $C|\mathbf{F}_q$ and the trace code $tr(C)$ are codes over $\mathbf{F}_q$. The next two theorems state that q-invariant codes have the same parameters as subfield subcodes. Therefore, we may work with q-invariant codes over $\mathbf{F}_{q^m}$.

Theorem 4.1.2 *Suppose C is code over $\mathbf{F}_{q^m}$. The following are equivalent.*

- *C is a q-invariant code,*
- *C has a basis of vectors in $\mathbf{F}_q^n$,*
- $\dim_{\mathbf{F}_{q^m}} C = \dim_{\mathbf{F}_q} C|\mathbf{F}_q$.

Theorem 4.1.3 *Suppose C is a q-invariant code over $\mathbf{F}_{q^m}$. Then, C is a $[n,k,d]_{\mathbf{F}_{q^m}}$ code if and only if $C|\mathbf{F}_q$ is an $[n,k,d]_{\mathbf{F}_q}$ code.*

Definition 4.1.4 *Let C be a code over $\mathbf{F}_{q^m}$. We define the following:*

$$C^0 := C \cap C^{(q)} \cap C^{(q^2)} \cap \ldots \cap C^{(q^{m-1})} \text{ and } C^\wedge := C + C^{(q)} + C^{(q^2)} + \cdots + C^{(q^{m-1})}.$$

Note that C^0 is the largest q-invariant subspace of C and $C^\wedge$ is the smallest q-invariant space containing C.

Lemma 4.1.5 *Let C be a code over $\mathbf{F}_{q^m}$. Then,*

$$C^0 = Span_{\mathbf{F}_{q^m}}(C|\mathbf{F}_q), C^\wedge = Span_{\mathbf{F}_{q^m}}(tr(C)) \text{ and } (C^0)^\perp = (C^\perp)^\wedge.$$

Delsarte's lemma, i.e. $(C|\mathbf{F}_q)^\perp = tr(C^\perp)$, follows effortlessly.

Now we present some results on the q-invariance of cyclic codes and graph codes. These theorems allow us to find graph codes using q-invariant component codes.

Theorem 4.1.6 *Let $S \subseteq \mathbb{Z}_{q^m-1}$. The set S is closed under multiplication* mod $q^m - 1$ *by q if and only if $C(\mathbf{F}_{q^m}^*, Span_{\mathbf{F}_{q^m}}(\{t^j \mid j \in S\}))$ is a q-invariant code.*

Proof.

Let $f \in Span_{\mathbf{F}_{q^m}}(\{t^j \mid j \in S\})) \subseteq \mathbf{F}_{q^m}[t]/\langle t^{q^m-1} - 1\rangle$. The function given by $f^q \mod t^{q^m-1} - 1 \in Span_{\mathbf{F}_{q^m}}(\{t^j \mid j \in S\})) \subseteq \mathbf{F}_{q^m}[t]/\langle t^{q^m-1} - 1\rangle$ if and only if S is closed under multiplication $\mod (q^m - 1)$ by q. □

This presentation of cyclic codes is related to the classical definition using roots of the generator polynomial as parity equations. Consider $ev_{\mathbf{F}_q^*}(t^i) \cdot ev_{\mathbf{F}_q^*}(t^j)$. Note that, $ev_{\mathbf{F}_q^*}(t^i) \cdot ev_{\mathbf{F}_q^*}(t^j) = 0$ if and only if $i + j \neq 0 \mod (q-1)$. Therefore, picking the monomials $\{t^j \mid j \in S\}$ is the same as picking the roots α^j, such that $f(\alpha^{-j}) = 0$ for $f \in \mathbf{F}_q[t]/\langle t^{q-1} - 1\rangle$. We chose the monomial representation of the cyclic code because it represents a cyclic code as an evaluation code over $V = \mathbf{F}_q^*$.

Theorem 4.1.7 *Let G be an (n_1, n_2)-regular endpoint labeled bipartite graph. Let C_1 be a code of length n_1 over $\mathbf{F}_{q^m}$ and C_2 is a code of length n_2 over $\mathbf{F}_{q^m}$. Then*

$$(G, C_1 : C_2)^0 = (G, C_1^0 : C_2^0) \text{ and } (G, C_1 : C_2)|\mathbf{F}_q = (G, C_1|\mathbf{F}_q : C_2|\mathbf{F}_q).$$

Proof.

The two equalities are equivalent, thus we will prove only the first one:

$$(G, C_1 : C_2)^0 = (G, C_1 : C_2) \cap (G, C_1 : C_2)^{(q)} \cap \ldots \cap (G, C_1 : C_2)^{(q^{m-1})},$$

but $(G, C_1 : C_2)^{(q)} = (G, C_1^{(q)} : C_2^{(q)})$. This implies

$$(G, C_1 : C_2)^0 = (G, C_1 : C_2) \cap (G, C_1^{(q)} : C_2^{(q)}) \cap \ldots \cap (G, C_1^{(q^{m-1})} : C_2^{(q^{m-1})}).$$

We apply the definition of a graph code to obtain

$$(G, C_1 : C_2)^0 = (G, C_1 \cap C_1^{(q)} \cap \ldots \cap C_1^{(q^{m-1})} : C_2 \cap C_2^{(q)} \cap \ldots \cap C_2^{(q^{m-1})}).$$

Therefore,

$$(G, C_1 : C_2)^0 = (G, C_1^0 : C_2^0).$$

□

4.2 Graph codes over Γ_{sub} with cyclic component codes

In this section we construct some Tanner codes with cyclic component codes. First, we define the graph and the affine variety we will be working with in this chapter, and then we discuss the parameters of some of these codes.

Definition 4.2.1 *We define* $V := \{(x, y, a, b) \in \mathbf{F}_q^4 \mid ax + b - y = 0, ax \neq 0\}$.

Note that each element $(x, y, a, b) \in V$ is determined by the values of x and a and either y or b, therefore $\#V = (q-1)^2 q$. Denote the lexicographical order with $B > A > X > Y$ by $\preceq_1$ and lex order with $Y > X > A > B$ by $\preceq_2$.

Theorem 4.2.2 *The set* $\{AX + B - Y, X^{q-1} - 1, Y^q - Y, A^{q-1} - 1, B^q - B\}$ *is a Gröbner basis for* $\boldsymbol{I}(V)$ *under both* $\preceq_1$ *and* $\preceq_2$.

Proof.

This ideal is closely related to the ideal of Example 2.3.22. We can prove the theorem with the same technique. Under $\preceq_1$ we have the leading monomials: $LM_{\preceq_1}(AX + B - Y) = B$, $LM_{\preceq_1}(X^{q-1} - 1) = X^{q-1}$, $LM_{\preceq_1}(Y^q - Y) = Y^q$, $LM_{\preceq_1}(A^{q-1} - 1) = A^{q-1}$ and $LM_{\preceq_1}(B^q - B) = B^q$. The footprint $\Delta_{\preceq_1}(\mathbf{I}(V))$ is contained in $\{X^i Y^l A^j \mid 0 \leq i, j \leq q-2,\ 0 \leq l \leq q-1\}$. However, since $\#V = (q-1)^2 q$, the footprint must be of this cardinality and therefore the two sets are the same. A similar proof holds for $\preceq_2$. □

For future reference we give the following corollary.

Corollary 4.2.3

$$\Delta_{\preceq_1}(\boldsymbol{I}(V)) = \{X^i Y^l A^j \mid 0 \leq i,j \leq q-2,\ 0 \leq l \leq q-1\}.$$
$$\Delta_{\preceq_2}(\boldsymbol{I}(V)) = \{X^i B^l A^j \mid 0 \leq i,j \leq q-2,\ 0 \leq l \leq q-1\}.$$

Definition 4.2.4 *We define the graph Γ_{sub} as the following bipartite graph. The vertex set $V_1(\Gamma_{sub}) := \{(x,y) \in \mathbf{F}_q^* \times \mathbf{F}_q \mid (x,y,a,b) \in V\}$. Likewise $V_2(\Gamma_{sub}) := \{(a,b) \in \mathbf{F}_q^* \times \mathbf{F}_q \mid (x,y,a,b) \in V\}$. The edge set $E(\Gamma_{sub})$ is defined as $\{((x,y),(a,b)) \in V_1(\Gamma_{sub}) \times V_2(\Gamma_{sub}) \mid (x,y,a,b) \in V\}$.*

Note that Γ_{sub} is a $(q-1,q-1)$ regular endpoint labeled bipartite graph. In this case, the sets S_1 and S_2 for the bijections are the affine variety $\mathbf{F}_q^* = V(t^{q-1}-1)$ as an affine variety of $\mathbb{A}(1,\mathbf{F}_q)$. We find $E((x,y)) = \{(x,y,a,y-ax) \mid a \in \mathbf{F}_q^*\}$. For $(a,b) \in V_2(\Gamma_{sub})$, the set $E((a,b)) = \{(x,ax+b,a,b) \mid x \in \mathbf{F}_q^*\}$ is also indexed by $\mathbf{F}_q^*$. We use this indexing by $\mathbf{F}_q^*$ in the endpoint labelings.

Definition 4.2.5 *The $(q-1,q-1)$-regular graph Γ_{sub} is a $(q-1,q-1)$-regular endpoint labeled bipartite graph with the following bijections.*

$$\begin{array}{lccccl}
\forall (a,b) \in V_2(\Gamma_{sub}) & \phi_{(a,b)}: & \mathbf{F}_q^* & \to & E((a,b)) \\
 & \phi_{(a,b)}(x) & & = & (x, ax+b, a, b) \\
\forall (x,y \in V_1(\Gamma_{sub}) & \chi_{(x,y)}: & \mathbf{F}_q^* & \to & E((x,y)) \\
 & \chi_{(x,y)}(a) & & = & (x, y, a, y-ax)
\end{array}$$

We define the following sets of equivalence classes of monomials.

Definition 4.2.6 *Let $S \subseteq \mathbb{Z}_{q-1}$, then*

$$\mathcal{M}_1(S) := \{X^i Y^l A^j + \boldsymbol{I}(V) \mid 0 \leq i \leq q-2,\ 0 \leq l \leq q-1,\ j \in S\},$$
$$\mathcal{M}_2(S) := \{X^i B^l A^j + \boldsymbol{I}(V) \mid 0 \leq j \leq q-2,\ 0 \leq l \leq q-1,\ i \in S\}.$$

A simple counting argument shows $\#\mathcal{M}_1(S) = \#\mathcal{M}_2(S) = q(q-1)\#S$. We remark that the elements of $\mathcal{M}_1(S)$ are equivalence classes of monomials in $\Delta_{\preceq_1}(\mathbf{I}(V))$. In the same manner, the elements of $\mathcal{M}_2(S)$ are equivalence classes of monomials in $\Delta_{\preceq_2}(\mathbf{I}(V))$.

Theorem 4.2.7 *Let $S \subseteq \mathbb{Z}_{q-1}$, then*

$$C(V, \mathcal{M}_1(S)) = (\Gamma_{sub}, C(\mathbf{F}_q^*, \mathcal{M}_t(S)) : \mathbf{F}_q^{q-1}),$$
$$C(V, \mathcal{M}_2(S)) = (\Gamma_{sub}, \mathbf{F}_q^{q-1} : C(\mathbf{F}_q^*, \mathcal{M}_t(S))).$$

PROOF.

Let $f(X,Y,A) \in Span_{\mathbf{F}_q}(\mathcal{M}_1(S))$. For $(x,y) \in V_1(\Gamma_{sub})$, we consider the equivalence class $f(x,y,A)$. Note that $f(x,y,A) \in Span_{\mathbf{F}_q}(\{A^j + \mathbf{I}(V) \mid j \in S\})$. This implies that we can also consider $f(x,y,A)$ as a polynomial $f_{xy}(A)$, such that $f_{x,y}(A) + \langle A^{q-1} - 1 \rangle \in Span_{\mathbf{F}_q}(\{A^j + \langle A^{q-1} - 1 \rangle \mid j \in S\})$. Therefore, f evaluates to a codeword in the component code $C(\mathbf{F}_q^*, \mathcal{M}_t(S))$. For the code position $\alpha \in \mathbf{F}_q^*$, the label corresponding to it, $\chi_{(x,y)}(\alpha)$, is the edge $(x, y, \alpha, y - \alpha x)$. Evaluating $f(x,y,A)$ at $A = \alpha$ is the same as evaluating $f(X,Y,A)$ at the edge $\chi_{(x,y)}(\alpha)$. Therefore, f evaluates to a codeword of $(\Gamma_{sub}, C(\mathbf{F}_q^*, \mathcal{M}_t(S)) : \mathbf{F}_q^{q-1})$. The size of $\mathcal{M}_1(S)$ is $q(q-1)\#S$. Since $\mathcal{M}_1(S)$ is a subset of $\Delta_{\preceq_1}(\mathbf{I}(V))$, the dimension of $C(V, \mathcal{M}_1(S))$ is $q(q-1)\#S$. Lemma 3.2.8 states that the auxiliary graph codes are isomorphic to the direct product of their nontrivial component code. Therefore, the dimension of $(\Gamma_{sub}, C(\mathbf{F}_q^*, \mathcal{M}_t(S)) : \mathbf{F}_q^{q-1})$ is also $q(q-1)\#S$, which implies the codes are equal. The second equality follows similarly. □

For $S_X, S_A \subseteq \mathbb{Z}_{q-1}$ we denote the code $(\Gamma_{sub}, C(\mathbf{F}_q^*, \mathcal{M}_t(S_X)) : C(\mathbf{F}_q^*, \mathcal{M}_t(S_A)))$ by $(\Gamma_{sub}, S_X : S_A)$. To find the codewords of $(\Gamma_{sub}, S_X : S_A)$ we need a way to compute $Span_{\mathbf{F}_q}(\mathcal{M}_1(S_X)) \cap Span_{\mathbf{F}_q}(\mathcal{M}_2(S_A))$. We give a closer look to the footprints $\Delta_{\preceq_1}(\mathbf{I}(V))$ and $\Delta_{\preceq_2}(\mathbf{I}(V))$.

DEFINITION 4.2.8

$$\mathcal{M}_1(i,j) := \{X^{i-s}A^{j-s}Y^s + \boldsymbol{I}(V) \mid s \in \mathbb{Z}_{q-1}\}.$$

$$\mathcal{M}_2(i,j) := \{X^{i-s}A^{j-s}Y^s + \boldsymbol{I}(V) \mid s \in \mathbb{Z}_{q-1}\}.$$

Where the negative powers of X and A are considered $\mod q-1$.

THEOREM 4.2.9 *In $\mathbf{F}_q[X,Y,A,B]/\boldsymbol{I}(V)$, for $0 \leq i,j \leq q-1$, the $\mathbf{F}_q$-vector spaces $Span_{\mathbf{F}_q}(\mathcal{M}_1(i,j))$ and $Span_{\mathbf{F}_q}(\mathcal{M}_2(i,j))$ are equal.*

PROOF.

Note that $\bar{f} \in \mathcal{M}_1(0,0)$ if and only if $(X^iA^j + \mathbf{I}(V))\bar{f} \in \mathcal{M}_1(i,j)$. There is a similar relation between $\mathcal{M}_2(0,0)$ and $\mathcal{M}_2(i,j)$. Thus we prove the statement only for the case $Span_{\mathbf{F}_q}(\mathcal{M}_1(0,0))$ and $Span_{\mathbf{F}_q}(\mathcal{M}_2(0,0))$. In this case,

$$\mathcal{M}_1(0,0) := \{X^{-s}A^{-s}Y^s + \mathbf{I}(V) \mid s \in \mathbb{Z}_{q-1}\},$$
$$\mathcal{M}_2(0,0) := \{X^{-s}A^{-s}B^s + \mathbf{I}(V) \mid s \in \mathbb{Z}_{q-1}\}.$$

Let $f \in Span_{\mathbf{F}_q}(\mathcal{M}_1(0,0))$. We write f as $\sum_{i=0}^{q-1} f_i(AX)^{q-1-i}Y^i + \mathbf{I}(V)$. Note that in $\mathbf{F}_q[X,Y,A,B]/\mathbf{I}(V)$ we have that $Y + \mathbf{I}(V)$ equals $(AX+B) + \mathbf{I}(V)$. Thus $f = \sum_{i=0}^{q-1} f_i(AX)^{q-1-i}(AX+B)^i + \mathbf{I}(V) = \sum_{i=0}^{q-1}(\sum_{j=i}^{q-1} f_j\binom{j}{i})(AX)^{q-1-i}B^i$. □

This allows us to compute the dimension of the graph codes simply by computing the intersections $\mathcal{M}_1(i,j) \cap \mathcal{M}_2(i,j)$ with Theorem 2.4.5 for all $0 \leq i,j \leq q-2$. To do this, we find the change of basis matrix from $\mathcal{M}_1(i,j)$ to $\mathcal{M}_2(i,j)$.

Definition 4.2.10 *Let U_q denote the $q \times q$ matrix whose entry at the i-th row and j-th column is $\binom{j}{i}$. The matrix U_q is known as* the Upper Pascal matrix.

From the proof of Theorem 4.2.9, we explicitly found U_q as the change of basis matrix from $\mathcal{M}_1(i,j)$ to $\mathcal{M}_2(i,j)$. Since we have a linear mapping from a basis of $\mathbf{F}_q[X,Y,A,B]/\mathbf{I}(V)$ to another basis of $\mathbf{F}_q[X,Y,A,B]/\mathbf{I}(V)$ mapping the disjoint spaces $\mathcal{M}_1(i,j)$ to the disjoint spaces $\mathcal{M}_2(i,j)$, we can find $Span_{\mathbf{F}_q}(\mathcal{M}_1(S_X)) \cap Span_{\mathbf{F}_q}(\mathcal{M}_2(S_A))$ by finding instead the intersection of the smaller spaces $Span_{\mathbf{F}_q}(\mathcal{M}_1(S_X) \cap \mathcal{M}_1(i,j)) \cap Span_{\mathbf{F}_q}(\mathcal{M}_2(S_A) \cap \mathcal{M}_2(i,j))$ for each of the possible $(q-1)^2$ values of (i,j).

4.3 Graph code parameters

In this section, we look at U_q, the change of basis matrix from $\mathcal{M}_1(i,j)$ to $\mathcal{M}_2(i,j)$, to find the dimension of graph codes with cyclic component codes. We focus on the case of Reed–Solomon component codes and p–invariant cyclic codes. We start with the following lemma:

Lemma 4.3.1 *Let $S_X, S_A \subseteq \mathbb{Z}_{q-1}$. For i and j, let $S'_X = \{s+j \mid s \in S_X\}$ be the shift of S_X by j and let $S'_A = \{s+i \mid s \in S_A\}$ be the shift of S_A by i. Then,*

$$(\Gamma_{sub}, S_X : S_A) \equiv (\Gamma_{sub}, S'_X : S'_A).$$

Proof.

Consider that $f + \mathbf{I}(V) \in \mathcal{M}_1(S_A) \cap \mathcal{M}_2(S_B)$ if and only if $x^j a^i f + \mathbf{I}(V)$ is in the code $\mathcal{M}_1(S'_X) \cap \mathcal{M}_2(S'_A)$. This implies $(\Gamma_{sub}, S_X : S_A)$ and $(\Gamma_{sub}, S'_X : S'_A)$. are monomially equivalent. □

4.3.1 Parameters of graph codes with Reed–Solomon component codes

We use the following theorem from [HJ11] and [RS06] to estimate the minimum distance of the graph codes over Γ_{sub}. We use the eigenvalues of the graph for one of the bounds. Since Γ_{sub} is $(q-1, q-1)$ regular, its largest eigenvalue is $q+1$. The second largest eigenvalue is $\sqrt{q}$. This follows from the fact that Γ_{sub} is a subgraph of the point–line incidence geometry of the projective plane over $\mathbf{F}_q$ and the eigenvalue interlacing theorem.

Theorem 4.3.2 *Let C_1 be a $[q-1, k_1, d_1]_{\mathbf{F}_q}$ code. Likewise, suppose C_2 is a $[q-1, k_2, d_2]_{\mathbf{F}_q}$ code. Let D denote the minimum distance of $(\Gamma_{sub}, C_1 : C_2)$. Then,*

$$D \geq d_1 d_2 + (d_1^2 - d_1)(d_2 - 1) \text{ and } q(q-1)\frac{d_1 d_2 - \sqrt{q d_1 d_2}}{q - 1 - \sqrt{q}}.$$

We have computationally verified for $q = 4, 8, 16, 32$ and 64 and $q = 9, 27$ and 81 that for $1 \leq k_x + k_a \leq q-1$

$$\dim(\Gamma_{sub}, RS(\mathbf{F}_q^*, k_x) : RS(\mathbf{F}_q^*, k_a)) \geq \frac{k_x k_a (k_x + k_a)}{2}.$$

We have also verified for $q - 1 \leq k_x + k_a \leq 2(q-1)$

$$\dim(\Gamma_{sub}, RS(\mathbf{F}_q^*, k_x) : RS(\mathbf{F}_q^*, k_a)) \geq$$

$$\frac{(q-k_x)(q-k_a)(2q-k_x-k_a)}{2} + (q^2-q)(k_x + k_a - (q-1)).$$

Theorem 4.3.2 shows that D is at least

$$(q-k_x)(q-k_a) + (q-k_x)(q-k_x-1)(q-k_a-1),$$

$$(q-k_x)(q-k_a) + (q-k_a)(q-k_a-1)(q-k_a-1),$$

$$\text{and } q(q-1)\frac{(q-k_x)(q-k_a) - \sqrt{q(q-k_x)(q-k_a)}}{q-1-\sqrt{q}}.$$

The bounds on the graph code parameters are sharp in some cases. We delve into the properties of binomial coefficients and U_q to later prove that the dimension bound is exact in several cases.

4.3.2 Parameters of graph codes with p–invariant cyclic component codes

Theorem 4.1.6 implies the cyclic code $C(\mathbf{F}_q^*, \mathcal{M}_t(S))$ is p-invariant if and only if S is closed under multiplication by p. In this section, we use p-invariant cyclic codes as component codes. Theorem 4.1.7 implies the resulting graph codes are the p-invariant codes of the graph codes of their subfield subcodes as component codes. Therefore the codes we present in this subsection have parameters over the subfield $\mathbf{F}_2$ and $\mathbf{F}_3$.

Please note that in this subsection we will represent the p-invariant sets S_X and S_A by a representative of each coset under the action of multiplying by p. For example, in the case that $q = 8$, we represent $\{0\}$ by $\{0\}$, $\{1, 2, 4\}$ by $\{1\}$ and $\{3, 5, 6\}$ by $\{3\}$.

4.3.2.1 Graph codes over $\mathbf{F}_2$ for $q = 8$, $N = 392$

S_X	S_A	k_x	d_x	k_a	d_a	K	$\geq D$
$\{0\}$	$\{0\}$	1	7	1	7	1	392
$\{0\}$	$\{1\}$	1	7	3	4	6	175
$\{0\}$	$\{3\}$	1	7	3	4	6	175
$\{0\}$	$\{0,1\}$	1	7	4	3	10	108
$\{0\}$	$\{0,3\}$	1	7	4	3	10	108
$\{0\}$	$\{1,3\}$	1	7	6	2	30	56
$\{1\}$	$\{1\}$	3	4	3	4	33	63
$\{3\}$	$\{1\}$	3	4	3	4	33	63
$\{3\}$	$\{3\}$	3	4	3	4	32	63
$\{1\}$	$\{0,1\}$	3	4	4	3	52	63
$\{1\}$	$\{0,3\}$	3	4	4	3	51	63
$\{3\}$	$\{0,1\}$	3	4	4	3	51	63
$\{3\}$	$\{0,3\}$	3	4	4	3	54	63
$\{0,1\}$	$\{0,1\}$	4	3	4	3	89	21
$\{0,3\}$	$\{0,1\}$	4	3	4	3	89	21
$\{0,3\}$	$\{0,3\}$	4	3	4	3	88	21

When $q = 8$ we can already see the importance of the labeling functions. In this case, there is an isomorphism between the cyclic codes of $\mathbf{F}_8^*$ obtained by the map $t \mapsto t^{-1}$. This means that the codes defined with the class of 1 and the codes defined with the class of 3 are isomorphic, yet the graph codes $(\Gamma_{sub}, \{1\} : \{1\})$ and $(\Gamma_{sub}, \{1\} : \{3\})$ have dimension 33 while $(\Gamma_{sub}, \{3\} : \{3\})$

has dimension 32. However, the dimension of $(\Gamma_{sub}, \{3\} : \{0,3\})$ is 54 and the dimension of $(\Gamma_{sub}, \{1\} : \{0,1\})$ is 52. The other two codes, $(\Gamma_{sub}, \{3\} : \{0,1\})$ and $(\Gamma_{sub}, \{1\} : \{0,3\})$ have dimension 51. These differences in the dimension do not appear when we have both the class of 1 and the class of 3 in the monomials of the cyclic code component codes as we show now.

S_X	S_A	k_x	d_x	k_a	d_a	K	$\geq D$
$\{1,3\}$	$\{0\}$	6	2	1	7	30	56
$\{1,3\}$	$\{1\}$	6	2	3	4	122	20
$\{1,3\}$	$\{3\}$	6	2	3	4	122	20
$\{1,3\}$	$\{0,1\}$	6	2	4	3	174	12
$\{1,3\}$	$\{0,3\}$	6	2	4	3	174	12
$\{1,3\}$	$\{1,3\}$	6	2	6	2	281	6

4.3.2.2 Graph codes over $\mathbf{F}_2$ for $q = 16$, $N = 3600$

In this case, the cyclotomic cosets are $\{0\}$, $\{1\} = \{1,2,4,8\}$, $\{3\} = \{3,6,12,9\}$, $\{5\} = \{5,10\}$ and $\{7\} = \{7,14,13,11\}$. Now $-\{1\} = \{-1,-2,-4,-8\}$. In $\mathbb{Z}_{15}$ the coset $\{-1,-2,-4,-8\}$ is equal to $\{7\}$. All other cyclotomic cosets are their own inverses.

We will focus on these 2-invariant component codes: $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{1\}))$ and $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{7\}))$, which are $[15,4,8]$ codes, the codes $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,1\}))$ and $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,7\}))$, which are $[15,5,7]$ codes and $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,1,5\}))$ and $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,7,5\}))$, which are $[15,7,5]$ codes. In the next table we present graph codes with isomorphic component codes, but completely different behaviors of the dimension in all three cases.

S_X	S_A	k_x	d_x	k_a	d_a	K	$\geq D$
$\{1\}$	$\{1\}$	4	8	4	8	62	456
$\{1\}$	$\{7\}$	4	8	4	8	62	456
$\{7\}$	$\{7\}$	4	8	4	8	59	456
$\{0,1\}$	$\{0,1\}$	5	7	5	7	137	301
$\{0,1\}$	$\{0,7\}$	5	7	5	7	137	301
$\{0,7\}$	$\{0,7\}$	5	7	5	7	137	301
$\{0,1,5\}$	$\{0,1,5\}$	7	5	7	5	395	105
$\{0,1,5\}$	$\{0,7,5\}$	7	5	7	5	387	105
$\{0,7,5\}$	$\{0,7,5\}$	7	5	7	5	379	105

Now we compare what happpens when we compare different, non isomorphic codes.

S_X	S_A	k_x	d_x	k_a	d_a	K	$\geq D$
$\{1\}$	$\{0,1\}$	4	8	5	7	94	392
$\{1\}$	$\{0,7\}$	4	8	5	7	92	392
$\{7\}$	$\{0,1\}$	4	8	5	7	94	392
$\{7\}$	$\{0,7\}$	4	8	5	7	92	392
$\{1\}$	$\{0,1,5\}$	4	8	7	5	152	264
$\{1\}$	$\{0,7,5\}$	4	8	7	5	148	264
$\{7\}$	$\{0,1,5\}$	4	8	7	5	152	264
$\{7\}$	$\{0,7,5\}$	4	8	7	5	148	264
$\{0,1\}$	$\{0,1,5\}$	5	7	7	5	229	203
$\{0,1\}$	$\{0,7,5\}$	5	7	7	5	229	203
$\{0,7\}$	$\{0,1,5\}$	5	7	7	5	227	203
$\{0,7\}$	$\{0,7,5\}$	5	7	7	5	229	203

The dimension is harder to predict in this case. Now we give some examples with codes which contain $\{3,6,12,9\}$ in their monomial set.

S_X	S_A	k_x	d_x	k_a	d_a	K	$\geq D$
$\{1\}$	$\{3\}$	4	8	4	6	38	328
$\{7\}$	$\{3\}$	4	8	4	6	38	328
$\{3\}$	$\{3\}$	4	6	4	6	35	186
$\{0,1\}$	$\{0,3\}$	5	7	5	3	95	105
$\{0,7\}$	$\{0,3\}$	5	7	5	3	100	105
$\{0,3\}$	$\{0,3\}$	5	3	5	3	85	21

In the first example, $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{3\}))$ is a component code. When the second component code is $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{1\}))$ or $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{7\}))$ the dimension is higher than the case where $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{3\}))$ is the other component code. When $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,3\}))$ is a component code, then we get a higher dimension with $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,3\}))$ than with $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{1\}))$ or $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{7\}))$. Moreover, the dimension when $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{1\}))$ is a component code is different from the dimension when $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{7\}))$ is the second component code. When both component codes are $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{1\}))$ or $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{7\}))$ or $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,1\}))$ or $C(\mathbf{F}_{16}^*, \mathcal{M}_t(\{0,7\}))$ the dimension is higher.

4.3.2.3 Optimal Codes

We found some optimal binary codes as Tanner codes Γ_{sub} with cyclic component codes. There are several ways of estimating the minimum distance of Tanner codes [Rot06, HJ11], but these methods were insufficient to compute the minimum distance of the code. We generated all codewords to find the

minimum distance of the Tanner codes described in the following table. Their optimality is given by [Gra07].

q	S_A	$(\Gamma_{sub}, C(\mathbf{F}_q^*, M_t(S_A)))$	Status
*	$\{1,2,4\}$	$[56,6,28]$	Optimal
8	$\{0,1,2,4\}$	$[56,10,24]$	Optimal
*	$\{1,2,4,8\}$	$[240,8,120]$	Optimal
16	$\{0,1,2,4,8\}$	$[240,13,112]$	Best Known

We also mention, for $q = 9$ and $S_A = \{0,1,3\}$ the code $(\Gamma_{sub}, C(\mathbf{F}_q^*, M_t(S_A)))$ is a $[72,5,45]_{\mathbf{F}_3}$ code where the optimal code is a $[72,5,46]_{\mathbf{F}_3}$ code.

Chapter 5

Graph Codes with Reed–Solomon Component Codes

The graphs introduced in this chapter are derived from the affine plane over $\mathbf{F}_q$. It turns out that the edge set of these graphs are affine varieties. We compute the dimension of the graph codes by considering them as affine variety codes.

We also introduce forcing sets. A forcing set for a graph G is defined only with combinatorial notions, but it allows us to encode a graph code iteratively provided the component codes are MDS codes. It also gives an upper bound on the dimension of a graph code with MDS component codes.

5.1 Graph code: $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$

Definition 5.1.1 *We denote the affine variety* $\{(x, y, a, b) \in \mathbf{F}_q^4 \mid ax+b = y\}$ *as a subvariety of* $\mathbb{A}(4, \mathbf{F}_q)$ *by* W.

Note that each point $(x, y, a, b) \in W$ is determined by the values of x and a

and either one of y or b, thus $\#W = q^3$. We denote degree graded reverse lexicographical order with $B > A > X > Y$ as $\preceq_1$ and degree graded reverse lexicographical order with $Y > X > A > B$ as $\preceq_2$. First we define the following:

Definition 5.1.2 *We define*

$$f_i^{(1)} := X^i(Y-B)^{q-i} - A^{q-1-i}(Y-B)$$

$$f_i^{(2)} := A^i(Y-B)^{q-i} - X^{q-1-i}(Y-B)$$

Theorem 5.1.3 *The set*

$$\{AX + B - Y, X^q - X, Y^q - Y, A^q - A, B^q - B, f_i^{(1)}, f_i^{(2)}, i = 1, 2, \ldots q-1\}$$

is a Gröbner basis for $\boldsymbol{I}(V)$ under both $\preceq_1$ and $\preceq_2$.

Proof.

This is a simple corollary from the footprint bound. This is also the ideal discussed in Example 2.3.22. □

Definition 5.1.4 *We define the graph Γ_1 as the following bipartite graph. The vertex set $V_1(\Gamma_1) := \mathbf{F}_q^2$. Likewise the vertex set $V_2(\Gamma_1) := \mathbf{F}_q^2$ The edge set $E(\Gamma_1)$ is defined as $\{((x,y),(a,b)) \in V_1(\Gamma_1) \times V_2(\Gamma_1) \mid (x,y,a,b) \in W\}$.*

Note that Γ_1 is a (q,q)-regular bipartite graph.

Definition 5.1.5 *We use the following bijections to make a (q,q)-regular endpoint labeled bipartite graph with Γ_1.*

$$\begin{array}{lccccl} \forall (a,b) \in V_2(\Gamma_1) & \phi_{(a,b)} : & \mathbf{F}_q^* & \to & E((a,b)) \\ & \phi_{(a,b)}(x) & & = & (x, ax+b, a, b) \\ \forall (x,y \in V_1(\Gamma_1) & \chi_{(x,y)} : & \mathbf{F}_q^* & \to & E((x,y)) \\ & \chi_{(x,y)}(a) & & = & (x, y, a, y - ax) \end{array}$$

Definition 5.1.6 *We define the following monomial sets in* $\mathbf{F}_q[X, Y, A, B]$

$$\begin{aligned}
\mathcal{M}_1(k)^{(X)} &:= \{Y^{i_2} A^{j_1} B^{j_2} \mid j_1 + j_2 < k, i_2 < q\}, \\
\mathcal{M}_1(k)^{(A)} &:= \{X^{i_1} Y^{i_2} B^{j_2} \mid j_2 < k, i_1 + j_2 < q, i_2 < q\}, \\
\mathcal{M}_2(k)^{(X)} &:= \{Y^{i_2} A^{j_1} B^{j_2} \mid i_2 < k, j_1 + i_2 < q, j_2 < q\}, \\
\mathcal{M}_2(k)^{(A)} &:= \{X^{i_1} Y^{i_2} B^{j_2} \mid i_1 + i_2 < k, j_2 < q\}, \\
\mathcal{M}_1(k) &:= \mathcal{M}_1(k)^{(X)} \cup \mathcal{M}_1(k)^{(A)}, \\
\mathcal{M}_2(k) &:= \mathcal{M}_2(k)^{(X)} \cup \mathcal{M}_2(k)^{(A)}.
\end{aligned}$$

One can check $\mathcal{M}_1(k) \subseteq \Delta_{\preceq_1}(\mathbf{I}(W))$ and $\mathcal{M}_2(k) \subseteq \Delta_{\preceq_2}(\mathbf{I}(W))$. A counting argument shows that for $1 \leq k \leq q$, both $\mathcal{M}_1(k)$ and $\mathcal{M}_2(k)$ have exactly $q^2 k$ monomials.

Now we use affine variety codes to study $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$. We can relate the auxiliary graph codes with the endpoint labeled graph Γ_1 to some affine variety codes over W.

Theorem 5.1.7

$$C(W, Span_{\mathbf{F}_q}(\mathcal{M}_1(k))) = (\Gamma_1, RS(\mathbf{F}_q, k) : \mathbf{F}_q^q)$$

$$C(W, Span_{\mathbf{F}_q}(\mathcal{M}_2(k))) = (\Gamma_1, \mathbf{F}_q^q : RS(\mathbf{F}_q, k))$$

Proof.

Let $f(X, Y, A, B) \in \langle \mathcal{M}_1(k) \rangle_{\mathbf{F}_q}$. For each $(x, y) \in V_1(\Gamma_1)$, we evaluate the univariate polynomial $f(x, y, A, y - Ax)$. From the bound on the degree of A and B, $f(x, y, A, y - Ax)$ is a polynomial of degree $< k$. Therefore f evaluates to a codeword in the component code $RS(\mathbf{F}_q, k)$. Now we need to ensure the code positions are the ones given by $\chi_{(x,y)}$. To the code position $\alpha \in \mathbf{F}_q$ we associate the edge $\chi_{(x,y)}(\alpha) = (x, y, \alpha, y - \alpha x)$. Evaluating $f(x, y, A, y - Ax)$ at $A = \alpha$ is the same value as evaluating $f(X, Y, A, B)$ at the edge $\chi_{(x,y)}(\alpha)$. Therefore $ev_W(f)$ is a codeword of $(\Gamma_1, RS(\mathbf{F}_q, k) : \mathbf{F}_q^q)$. The dimension of $Span_{\mathbf{F}_q}(\mathcal{M}_1(k))$ is $q^2 k$. Since $\mathcal{M}_1(k) \subseteq \Delta_{\preceq_1}(\mathbf{I}(W))$, the dimension of $C(W, Span_{\mathbf{F}_q}(\mathcal{M}_1(k)))$ is also $q^2 k$. The dimension of $(\Gamma_1, RS(\mathbf{F}_q, k) : \mathbf{F}_q^q)$ is also $q^2 k$ which implies both codes are the same. The other equality follows in a similar manner. □

Definition 5.1.8 *Let*

$$\{f \in \mathcal{M}_1(k) \mid \exists\, g \in \mathcal{M}_2(k) \ : \ f - g \in \boldsymbol{I}(W)\} = Span_{\mathbf{F}_q}(f_1, f_2, \ldots, f_s)$$

as an $\mathbf{F}_q$*-linear space and*

$$N_k := Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k)) \cap \boldsymbol{I}(W).$$

Theorem 5.1.9 *The graph code* $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ *is the affine variety code* $C(W, Span_{\mathbf{F}_q}(f_1, f_2, \ldots, f_s))$.

Proof. The proof follows from Theorem 2.4.6 and Theorem 5.1.7. □

Theorem 5.1.10 *If* $1 \leq k \leq \frac{q}{2}$*, the dimension of* $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ *is least* k^3*. If* $\frac{q}{2} \leq k \leq q$*, then the dimension of* $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ *is at least* $k^3 - 3q^2k + q^2k$.

Proof.

If $1 \leq k \leq \frac{q}{2}$ the linear space $Span_{\mathbf{F}_q}(f_1, f_2, \ldots, f_s)$ has at least the k^3 independent monomials in $\mathcal{M}_1(k) \cap \mathcal{M}_2(k)$. These k^3 monomials and Theorem 5.1.9 imply that $\dim(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k)) \geq k^3$. For $\frac{q}{2} \leq k \leq q$ Corollary 3.2.11 implies that $\dim(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ is at least $k^3 - 3q^2k + q^2k$. □

To find the dimension of the graph codes $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$, we must find the dimension of the space $N_k = \mathbf{I}(W) \cap Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$. When $N_k = \{0\}$ then a basis of $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$, would be given by the evaluation of the monomials in $\mathcal{M}_1(k) \cap \mathcal{M}_2(k)$. We will prove that in some cases $N_k = \{0\}$. We describe the proof as follows.

We first define a set of elements of $\mathbf{I}(W)$ which turn out to generate the $\mathbf{F}_q$-linear space $\mathbf{I}(W) \cap Span_{\mathbf{F}_q}(\Delta_{\preceq_1}(\mathbf{I}(W)) \cup \Delta_{\preceq_2}(\mathbf{I}(W)))$. Then we partition these ideal elements into subspaces, such that different spaces have disjoint support. We then prove that if an ideal element is in $\mathbf{I}(W) \cap Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$, then it is an $\mathbf{F}_q$-linear combination of some disjoint spaces. We then prove that if a polynomial in a subspace is also in $\mathbf{I}(W) \cap Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$, then certain matrices of binomial coefficients must have a nonzero element in its right kernel. We finish by proving that these binomial matrices have full rank, which implies that $\mathbf{I}(W) \cap Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k)) = \{0\}$.

Definition 5.1.11 *Let* $M \in \Delta_{\preceq_1}(\boldsymbol{I}(W))$*. We define*

$$f_M := M - rem_{\preceq_2}(M).$$

Lemma 5.1.12

$$\boldsymbol{I}(W) \cap Span_{\mathbf{F}_q}(\Delta_{\preceq_1}(\boldsymbol{I}(W)) \cup \Delta_{\preceq_2}(\boldsymbol{I}(W))) =$$
$$Span_{\mathbf{F}_q}(\{f_M | M \in \Delta_{\preceq_1}(\boldsymbol{I}(W)) \setminus \Delta_{\preceq_2}(\boldsymbol{I}(W))\}).$$

Proof.

If $f \in \mathbf{I}(W) \cap Span_{\mathbf{F}_q}(\Delta_{\preceq_1}(\mathbf{I}(W)) \cup \Delta_{\preceq_2}(\mathbf{I}(W)))$, then $f = g - rem_{\preceq_2}(g)$ for some $g \in Span_{\mathbf{F}_q}(\Delta_{\preceq_1}(\mathbf{I}(W)))$. If $g = \sum\ g_M\ M$, then $f = \sum g_M\ f_M$. The reverse containment follows from the definition of f_M. □

Lemma 5.1.13

$$N_k \subseteq \boldsymbol{I}(W) \cap Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \Delta_{\preceq_2}(\boldsymbol{I}(W))).$$

Now we shall find the dimension of N_k which will give the dimension of the graph codes. To do this, we exploit the structure of the ideal elements f_M. We can compute f_M explicitly. However, we only need the following facts: if $M = X^{i_1} Y^{i_2} B^{j_2}$, then

$$f_M = X^{i_1} f_1(Y, B) + X^{i_1} f_2(Y, B) + A^{q-1-i_1} f_3(Y, B) \tag{5.1}$$

where f_1, f_2 and f_3 are homogeneous polynomials in Y and B of degrees $i_2 + j_2$, $i_2 + j_2 - (q-1)$ and $i_2 + j_2 + i_1 - q + 1$ respectively and f_2 is a multiple of B. Furthermore,

$$f_1(Y, B) + B^{q-i_1} f_2(Y, B) = q_{i_2, q-i_1}(Y, B)(Y - B)^{q-i_1} \tag{5.2}$$

Likewise if $M = A^{j_1} Y^{i_2} B^{j_2}$, then

$$g_M = A^{j_1} g_1(Y, B) + A^{j_1} g_2(Y, B) + X^{q-1-j_1} g_3(Y, B) \tag{5.3}$$

where g_1, g_2 and g_3 are homogeneous polynomials in Y and B of degrees $i_2 + j_2$, $i_2 + j_2 - (q-1)$ and $i_2 + j_2 + j_1 - q + 1$ respectively and g_2 is a multiple of B. Furthermore,

$$g_1(Y, B) + B^{q-1} g_2(Y, B) = q_{i_2, q-j_1}(Y, B)(Y - B)^{q-j_1} \tag{5.4}$$

where $q_{i,j}(Y, B)$ is a homogeneous polynomial in Y and B of degree $i - j$.

Definition 5.1.14 *We denote by $\mathcal{M}_1(k)^{(1)}_{i,a}$ as the subset of $\mathcal{M}_1(k)$ of monomials M satisfying $deg_X\ M = i$, $deg_B\ M + deg_Y\ M = a$. Likewise we denote by $\mathcal{M}_1(k)^{(2)}_{i,a}$ as the subset of $\mathcal{M}_1(k)$ of monomials M satisfying $deg_A\ M = i$, $deg_B\ M + deg_Y\ M = a$.*

The sets $\mathcal{M}_1(k)^{(1)}_{i,a}$ and $\mathcal{M}_1(k)^{(2)}_{i,a}$ allow us to partition N_k into subspaces of polynomials with disjoint support. This separation will help us in finding the elements, if any, of N_k.

Lemma 5.1.15 *Let S_1, S_2 be two distinct subsets of the form $\mathcal{M}_1(k)^{(1)}_{i,a}$ or $\mathcal{M}_1(k)^{(2)}_{i,a}$ as in Definition 5.1.14 where $i < k \leq q/2$. Suppose that the polynomial $f = \sum_{M \in S_1} c_M f_M$ and $g = \sum_{M \in S_2} d_M f_M$. Then f and g have disjoint support.*

Proof.

If $M \in S_1 = \mathcal{M}_1(k)^{(1)}_{i_1,a}$, then equation (5.1) implies that f can be written as $X^{i_1} f_4(Y,B) + X^{i_1} f_5(Y,B) + A^{q-1-i_1} f_6(Y,B)$ where f_4, f_5 and f_6 are homogeneous polynomials in Y and B of degrees a, $a-(q-1)$ and $a+i_1-q+1$ respectively. If $S_2 = \mathcal{M}_1(k)^{(1)}_{i_1',a'}$ and either $i_1' \neq i_1$ or $a \neq a'$ then g has no term in its support in common with f. Therefore we assume $S_2 = \mathcal{M}_1(k)^{(2)}_{j_1,a'}$. However, equation (5.3) implies $q-1-i_1 = j_1$. The hypothesis of the lemma states $j_1 < k$. However, since $j_1 + i_1 = q-1$, $j_1 > q-1-k \geq q/2$, then f and g have disjoint support. Similarly, the case $S_1 = \mathcal{M}_1(k)^{(2)}_{j_1,a}$ follows. □

Lemma 5.1.16 *Suppose $f \in Span_{\mathbf{F}_q}(f_M)$, $M \in \mathcal{M}_1(k)^{(1)}_{i_1,a}$. Furthermore suppose f equals $X^{i_1} f_4(Y,B) + X^{i_1} f_5(Y,B) + A^{q-1-i_1} f_6(Y,B)$ where f_4, f_5 and f_6 are homogeneous polynomials in Y and B of degrees a, $a-(q-1)$ and $a+i_1-q+1$. If $f \in Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$, then $f_4(Y,B) + B^{q-1} f_5(Y,B)$ is a multiple of $(Y-B)^{q-i_1}$, whose terms satisfy either $deg_B \geq q$ or $deg_B < k$.*

Proof.

Equation (5.2) implies that $f_4(Y,B) + B^{q-1} f_5(Y,B)$ is a homogeneous polynomial and a multiple of $(Y-B)^{q-i_1}$. We write $f_4(Y,B) + B^{q-1} f_5(Y,B)$ as $h(Y,B)(Y-B)^{q-i_1}$. Since $X^{i_1}(f_4(Y,B) + f_5(Y,B)) \in Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$, the polynomial $h(Y,B)$ has the desired properties. □

LEMMA 5.1.17 *Suppose* $f \in Span_{\mathbf{F}_q}(f_M)$, $M \in \mathcal{M}_1(k)^{(2)}_{j_1,a}$. *Furthermore suppose* f *equals* $A^{j_1}g_4(Y,B) + A^{j_1}g_5(Y,B) + X^{q-1-j_1}g_6(Y,B)$ *where* g_4, g_5 *and* g_6 *are homogeneous polynomials in* Y *and* B *of degrees* a, $a-(q-1)$ *and* $a+j_1-q+1$. *If* $f \in Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$, *then* $g_4(Y,B) + B^{q-1}g_5(Y,B)$ *is a multiple of* $(Y-B)^{q-j_1}$, *whose terms satisfy either* $deg_B \geq q$ *or* $deg_B < k - j_1$.

PROOF. The proof is the same as in Lemma 5.1.16. □

Lemma 5.1.16 shows that a nonzero element of N_k gives rise to a multiple of $(Y-B)^{q-i_1}$ with no monomials in the middle. We will show that in the cases relevant to $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ there does not exist a multiple of $(Y-B)^l$ such that we find a nonzero element of $\mathbf{I}(W)$ in $Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cup \mathcal{M}_2(k))$. This will give a closed formula for the dimension in these cases.

LEMMA 5.1.18 *Let* $h(Y,B) = \sum_{j=0}^{m} h_j Y^j B^{m-j}$. *The homogeneous polynomial* $h(Y,B)(Y-B)^l$ *can be written as a polynomial whose terms have either degree in* B *less than* d_1 *or degree in* B *greater than* d_2 *if and only if the coefficient vector* $\boldsymbol{h} = (h_m, h_{m-1}, \ldots, h_0)$ *is in the left kernel of* $F = (\binom{l}{d_1-v+u})_{0 \leq u \leq d_2-d_1, 0 \leq v \leq m}$.

PROOF.

The vector $\mathbf{h}F$ represents the coefficients of $h(Y,B)(Y-B)^l$ which do not satisfy the degree conditions from the theorem. These terms are 0 if and only if $\mathbf{h}$ is in the left kernel of F. □

DEFINITION 5.1.19 *Let* k, h, r *be integers. We define*

$$B(k,h,r) := \left(\binom{k}{r+h-v+u} \right)_{0 \leq u,v \leq h}.$$

LEMMA 5.1.20 *Let* $m \geq 1$, $i < 2^{m-1}$, $0 \leq h \leq i-1$, *then the matrix of binomial coefficients* $B(2^m - i, h, 2^{m-1} - h)$ *has full rank over* $\mathbf{F}_{2^m}$.

PROOF.

Since $i < 2^{m-1}$, Lucas' Lemma [Luc78] implies $\binom{2^m-i}{2^{m-1}} = 1$. Therefore the entries on the main diagonal $u - v = 0$ are equal to 1. If $0 < v - u \leq h$, then $2^m - i < 2^{m-1} - (v-u) < 2^{m-1}$. Similarly, the entries below the main diagonal are 0. Therefore, the determinant of $B(2^m - i, h, 2^{m-1} - h)$ is 1. □

Lemma 5.1.21 *Let $q = 2^m$. Suppose $k \leq 2^{m-1}$. Then $N_k = \{0\}$.*

Proof.

Let $h < i_1 < k$. Let $g(Y, B)$ be a homogeneous polynomial of degree h such that no term, M, of $g(Y, B)(Y - B)^{q-i_1}$ satisfies $k \leq deg_B\ M < q$. This implies the matrix $(\binom{q-i_1}{k-v+u})_{0\leq u\leq q-1-k, 0\leq v\leq h}$ has a nonzero left kernel element. However, $B(q - i, h, k - h)$ is a submatrix, Lemma 5.1.20 implies it has full rank. □

Lemma 5.1.22 *Let $q = p$, p a prime. Suppose $k \leq \frac{p}{2}$. Then $N_k = \{0\}$.*

Proof.

Let $h < i_1 < k$. Let $g(Y, B)$ be a homogeneous polynomial of degree h such that no term, M, of $g(Y, B)(Y - B)^{p-i_1}$ satisfies $k \leq deg_B\ M < p$. This implies the matrix $(\binom{p-i_1}{k-v+u})_{0\leq u\leq p-1-k, 0\leq v\leq h}$ has a nonzero left kernel element. However, $B(p - i, h, k - h)$ is a submatrix. [Mat08] states that it has full rank. □

We have proved that in certain cases there are no nonzero ideal elements in N_k. In this way we obtain the following dimensions for the following graph codes.

Theorem 5.1.23 *Let q equal a power of 2 or a prime. Then,*

$$\text{If } 1 \leq k \leq \frac{q}{2}, \text{ then } \dim(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k)) = k^3.$$

$$\text{If } \frac{q}{2} \leq k \leq q, \text{ then } \dim(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k)) = k^3 - 3q^2k + q^2k.$$

Proof.

Lemmas 5.1.21 and 5.1.22 imply that when q satisfies the conditions of the theorem and $k \leq q/2$, then $N_k = \{0\}$. Therefore, the $\mathbf{F}_q$-linear vector space $\{f \in \mathcal{M}_1(k) \mid \exists\, g \in \mathcal{M}_2(k)\ :\ f - g \in \mathbf{I}(W)\}$ is equal to $Span_{\mathbf{F}_q}(\mathcal{M}_1(k) \cap \mathcal{M}_2(k))$. Thus, $\dim(\Gamma, RS(k) : RS(k)) = k^3$. Corollary 3.2.11 implies the statement of the theorem for $\frac{q}{2} \leq k \leq q$. □

Generally, Theorem 5.1.23 does not hold. When q is an odd prime power, and the rate of the component codes is around $1/2$, then the dimension of the graph codes

is greater than k^3. For example, in the case $q = 9$ and $k = 4$, the dimension of the graph code $(\Gamma_1, RS(\mathbf{F}_9, 4) : RS(\mathbf{F}_9, 4))$ is $66 > 4^3$. The polynomial $(Y - B)^6$ over $\mathbb{F}_3$ equals $Y^6 + B^3Y^3 + B^6$. With this polynomial we find the ideal elements $X^3(Y - B)^6 - A^5(Y - B)$ and $A^3(Y - B)^6 - X^5(Y - B)$ are in the linear space $Span_{\mathbf{F}_9}\mathcal{M}_1(4) \cup \mathcal{M}_2(4))$. These ideal elements give two codewords which are not monomials in $\mathcal{M}_1(4) \cap \mathcal{M}_2(4)$. For example $X^3Y^6 + X^3Y^3B^3 \in \mathcal{M}_1(4)$ and $-X^3B^6 - A^5Y + A^5B \in \mathcal{M}_2(4)$ are two polynomals which evaluate to the same nonmonomial function. However, k^3 still is a useful lower bound on the dimension of $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$.

5.1.1 Parameters of $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$

We use the following theorem from [HJ11] and [RS06] to estimate the minimum distance of the graph codes $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$.

Theorem 5.1.24 *The minimum distance, D, of $(\Gamma_1, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$, satisfies the following:*

- $D \geq (q - k + 1)((q - k + 1)^2 - (q - k))$.
- $D \geq q^2(q - k + 1)\frac{q-k+1-\sqrt{q}}{q-\sqrt{q}}$.

For the case where $q = 4$ and $k = 2$, the bounds on the minimum distance are $D \geq 3^2 + (3^2 - 2) = 16$ and $D \geq 16 * 3 * \frac{1}{2} = 24$. A direct computation shows $D = 35$. The bound $D \geq 24$ may not be improved because it is a bound which depends only on the graph Γ_1 and the component code $RS(\mathbf{F}_q, k)$ and the bound is sharp because there is a graph code over Γ_1 with another labeling and $RS(\mathbf{F}_4, 2)$ as component code with parameters $[64, 10, 24]_{\mathbf{F}_4}$. We tried to improve the bound with a technique derived from the footprint bound as given in [Gei08]. However, in this case, the bound is $D \geq 21$.

For the case where $q = 4$ and $k = 3$, the bounds on the minimum distance are $D \geq 2^2 + (2^2 - 2) = 6$ and $D \geq 16 * 2 * \frac{0}{2} = 0$. A direct computation shows $D = 6$. The bound $D \geq 6$ may not be improved as the graph code is a $[64, 31, 6]_{\mathbf{F}_4}$*code*. We also considered the bound given by a different technique derived from the footprint bound as in [Gei08]. However, in this case, the bound is $D \geq 4$.

5.2 Graph code: $(\Gamma_2, RS(\mathfrak{I}, k) : RS(\mathfrak{I}, k))$

Definition 5.2.1 *We define* $U := \{(x, y, t) \in \mathbf{F}_{q^2}^3 \mid t^q + t = 1,\ xy = t\}$ *as an affine variety of* $\mathbb{A}(3, \mathbf{F}_{q^2})$. *We denote the affine variety* $\boldsymbol{V}(t^q + t - 1)$ *by* $\mathfrak{I}$ *as an affine variety of the line* $\mathbb{A}(1, \mathbf{F}_{q^2})$.

Note that each point $(x, y, t) \in U$ is determined by the values of x and t. For any $x \in \mathbf{F}_{q^2}^*$ there are q possible values of t. Once x and t are fixed, so is y. Therefore $\#U = q(q^2 - 1)$.

Definition 5.2.2 *We define the graph* Γ_2 *as the following bipartite graph. The vertex set* $V_1(\Gamma_2) := \mathbf{F}_{q^2}^*$ *Likewise the vertex set* $V_2(\Gamma_2) := \mathbf{F}_{q^2}^*$ *We define the edge set of* Γ_2 *as the set* $E(\Gamma_2) := \{(x, y) \in V_1(\Gamma_2) \times V_2(\Gamma_2) \mid (x, y, t) \in U\}$.

Note that Γ_2 is a (q, q)-regular bipartite graph.

Definition 5.2.3 *Let* $\preceq_1$ *be lexicographical order with* $Y > X > T$. *Likewise we denote by* $\preceq_2$ *the lexicographical order where* $X > Y > T$.

Theorem 5.2.4 *The ideal* $\boldsymbol{I}(U)$ *is generated by the polynomials* $T^q + T - 1$, $X^{q^2-1} - 1$, $Y^{q^2-1} - 1$ *and* $T - XY$.

Proof.

A quick check of the footprint of $\langle T^q + T - 1, X^{q^2-1} - 1, Y^{q^2-1} - 1, T - XY\rangle$ under $\preceq_1$ shows the footprint of the ideal has $q(q^2 - 1)$ elements. Since the basis elements evaluate to 0 at the points of U and U has $q(q^2 - 1)$ points, the equality follows. □

From this basis for $\mathbf{I}(U)$ we can easily find its Gröbner bases under $\preceq_1$ and $\preceq_2$.

Theorem 5.2.5 *The set* $\{T^q + T - 1, X^{q^2-1} - 1, Y - TX^{q^2-2}\}$ *is a Gröbner basis for* $\boldsymbol{I}(U)$ *under* $\preceq_1$, *and* $\{T^q + T - 1, Y^{q^2-1} - 1, X - TY^{q^2-2}\}$ *is a Gröbner basis for* $\boldsymbol{I}(U)$ *under* $\preceq_2$.

Proof.

The polynomial $Y = TX^{q^2-2}$ belongs to $\mathbf{I}(U)$. Since the ideal $\mathbf{I}(U)$ contains $T^q + T - 1$, $Y - TX^{q^2-2}$ and $X^{q^2-1} - 1$, the monomials T^q, X^{q^2-1} and Y can

not be in $\Delta_{\preceq_1}(\mathbf{I}(U))$. This implies $\#\Delta_{\preceq_1}(\mathbf{I}(U)) \leq q(q^2-1)$. Since U has at least $q(q^2-1)$ elements, the equality $\#\Delta_{\preceq_1}(\mathbf{I}(U)) = \#U$ follows, which implies $\{T^q + T - 1, Y - TX^{q^2-2}, X^{q^2-1} - 1\}$ is a Gröbner basis under $\preceq_1$. The case for $\preceq_2$ is similar. □

Definition 5.2.6 *To construct graph codes over Γ_2 we will use the following endpoint labelings:*

$$\chi_X(X, Y) := XY$$

$$\phi_Y(X, Y) := XY$$

Note that the edges of $E(\Gamma_2)$ represent the pair (X, Y) when $(X, Y, T) \in U$. We may represent the pair (X, Y) as $(X, \frac{T}{X})$ or $(\frac{T}{Y}, Y)$. Therefore, we may consider the labelings in the following equivalent way.

Theorem 5.2.7

$$\chi_X(X, \frac{T}{X}) = \chi_{\frac{T}{Y}}(\frac{T}{Y}, Y) := T$$

$$\phi_{\frac{T}{X}}(X, \frac{T}{X}) = \phi_Y(\frac{T}{Y}, Y) := T$$

The component codes we will be working with are $RS(\mathfrak{I} \subseteq \mathbf{F}_{q^2}, k)$. Since the positions of the component codes are indexed by the elements of $\mathfrak{I}$, the labelings map the edges of Γ_2 to $\mathfrak{I}$. We remark that the code $RS(\mathfrak{I} \subseteq \mathbf{F}_{q^2}, k)$ is actually the code $RS(\mathbf{F}_q, k)$ over the field $\mathbf{F}_{q^2}$. If $\eta \in \mathbf{F}_{q^2}$ is a zero of $T^q + T = 1$ and $\epsilon \in \mathbf{F}_{q^2}$ is a zero of $T^q + T = 0$ then all zeroes of $T^q + T = 1$ are of the form $\eta + \alpha\epsilon, \alpha \in \mathbf{F}_q$. Therefore, there is a bijection between $\mathfrak{I}$ and $\mathbf{F}_q$ by mapping $\eta + \alpha\epsilon$ to α. The binomial theorem gives a mapping from $Span_{\mathbf{F}_{q^2}}(1, z, z^2, \ldots, z^{k-1})$ to $Span_{\mathbf{F}_{q^2}}(1, \eta + z\epsilon, (\eta + z\epsilon)^2, \ldots, (\eta + z\epsilon)^{k-1})$ which gives the equality between $RS(\mathfrak{I} \subseteq \mathbf{F}_{q^2}, k)$ and $RS(\mathbf{F}_q, k)$.

Definition 5.2.8 *We define $\mathcal{M}_1(k), \mathcal{M}_2(k) \subseteq \mathbf{F}_{q^2}[X, Y, T]$ as follows:*

$$\mathcal{M}_1(k) := \{X^i T^j \mid 0 \leq i \leq q^2 - 2, 0 \leq j \leq k - 1\},$$

$$\mathcal{M}_2(k) := \{Y^i T^j \mid 0 \leq i \leq q^2 - 2, 0 \leq j \leq k - 1\}.$$

Note that $\mathcal{M}_1(k)$ is a subset of $\Delta_{\preceq_1}(\mathbf{I}(U))$ and $\mathcal{M}_2(k)$ is a subset of $\Delta_{\preceq_2}(\mathbf{I}(U))$.

As before, we relate the auxiliary graph codes with some affine variety codes.

Theorem 5.2.9

$$C(U, \mathcal{M}_1(k)) = (\Gamma_2, RS(\mathfrak{I}, k) : \mathbf{F}_{q^2}^q)$$

$$C(U, \mathcal{M}_2(k)) = (\Gamma_2, \mathbf{F}_{q^2}^q : RS(\mathfrak{I}, k))$$

Proof.

Let $f(X,T) \in Span_{\mathbf{F}_{q^2}}(\mathcal{M}_1(k))$. Fix $x \in \mathbf{F}_{q^2}^*$. Then $f(x,T)$ is a polynomial of degree at most $k-1$ in T. Let $t^q+t=1$, then t is equal to xy where $(x,y,t) \in U$. The position of $f(x,T)$ at $T = t$ is the one given by $\chi_X(X, \frac{T}{X})$. Therefore, $f(X,T)$ evaluated in the affine variety U is also codeword of $(\Gamma_1, RS(\mathfrak{I}, k) : \mathbf{F}_{q^2}^q)$. Since $\mathcal{M}_1(k)$ is a subset of the footprint, the dimension of the code $C(\Gamma_2, \mathcal{M}_1(k))$ is equal to $(q^2-1)k$ which is the same as the dimension of $(\Gamma_1, RS(\mathfrak{I}, k) : \mathbf{F}_{q^2}^q)$. The second equality follows similarly. □

Lemma 5.2.10 *Let $X^iT^j \in \mathcal{M}_1(k)$. Then,*

$$rem_{\preceq_2}(X^iT^j) = Y^{q^2-1-i}T^{i+j} \mod T^q + T - 1.$$

Proof.

We divide the monomial X^iT^j by $X = TY^{q^2-2}$ to obtain $Y^{q^2-1-i}T^{i+j}$ as the remainder of X^iT^j. Then the only possible leading term of T^q+T-1, $Y^{q^2-1}-1$, or $X - TY^{q^2-2}$ which might divide $Y^{q^2-1-i}T^{i+j}$ is T^q, therefore $rem_{\preceq_2}(X^iT^j)$ is equal to $Y^{q^2-1-i}T^{i+j} \mod (T^q + T - 1)$. □

Definition 5.2.11 *For $i = 0, 1, \ldots q^2-2$ We define*

$$\Delta_{\preceq_1}(\boldsymbol{I}(U))(i) := \{X^iT^j \ 0 \le j \le q-1\}$$

$$\Delta_{\preceq_2}(\boldsymbol{I}(U))(i) := \{Y^iT^j \ 0 \le j \le q-1\}.$$

The remainder induces a bijection between the spaces $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_1}(\mathbf{I}(U))(i))$ and $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_2}(\mathbf{I}(U))(q^2-1-i \mod q^2-1))$. Note that in the case $i=0$ the vector space $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_1}(\mathbf{I}(U))(0))$ is equal to $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_2}(\mathbf{I}(U))(0))$. To simplify notation we write $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_2}(\mathbf{I}(U))(q^2-1-i))$ instead. The bijection is given by $X^ih(T) \mapsto Y^{q^2-1-i}(T^ih(T) \mod T^q + T - 1)$. The key to computing the remainder lies in computing $h(T) \mod T^q + T - 1$. First, we arrange all remainders in a $(q^2-1) \times q$ matrix.

Definition 5.2.12 *Let R denote the following $q^2-1 \times q$ matrix. We denote by $r_{i,j}$ its (i,j)-th entry, which is defined as follows:*

$$\sum_{j=0}^{q-1} r_{i,j} T^j = T^i \mod T^q + T - 1.$$

It turns out that we can compute the entries of R.

Theorem 5.2.13 *Let $r_{i,j}$ denote the (i,j)-th entry of R. Then*

$$r_{i_1 q+i_0,j} = \begin{cases} (-1)^{j-i_o}\binom{i_1}{j-i_0} & 0 \le i_0 \le q-1-i_1,\ j \neq 0 \\ (-1)^{q-i_0}\binom{i_1}{q-i_0} & j = 0 \\ (-1)^{j+q-i_0}\binom{i_1+1}{j+q-i_0} & q-i_1 \le i_0 \le q-1\ j \neq 0 \end{cases}$$

Proof.

Let $i = i_1 q$. In this case the remainder of $T^i = (T^q)^{i_1} \mod T^q + T - 1$ is $(1-T)^{i_1}$. If $i_0 = 1, 2, \ldots q-1-i_1$, then $T^{i_0}(1-T)^{i_1}$ has degree less than q and the remainder coefficient is $r_{i_1 q+i_0,j} = (-1)^{j-i_0}\binom{i_1}{j-i_0}$. Now, suppose i_0 is one of $q-i_1, q-i_1+2, \ldots q-1$. We will compute the $i_1 q + i_0$-th row, from the previous row. For $2 \le j \le q-1$, the entry $r_{i_1 q+i_0,j}$ is equal to $r_{i_1 q+i_0-1,j-1}$, the entry $r_{i_1 q+i_0,0} = r_{i_1 q+i_0-1,q-1} = (-1)^{q-i_0}\binom{i_1}{q-i_0}$ and the entry corresponding to the column $j=1$ is $r_{i_1 q+i_0,1} = (-1)^{q-i_0+1}\binom{i_1+1}{q-i_0}$ which is equal to the difference $r_{i_1 q+i_0-1,0} - r_{i_1 q+i_0-1,q-1} = (-1)(-1)^{q-i_0-1}\binom{i_1}{q-i_0-1} + (-1)^{q-i_0}\binom{i_1}{q-i_0}$. □

As a consequence of the definition of R we have the following characterization of R.

Corollary 5.2.14 *Let R_i be the $q \times q$ submatrix of R obtained by taking q consecutive rows of R starting from i and cycling back to 0 if necessary. Then R_i is the change of basis matrix which maps $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_1}(\boldsymbol{I}(U))(i))$ to $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_2}(\boldsymbol{I}(U))(q^2-1-i))$.*

Proof.

If $X^i h(T) \in Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_1}(\mathbf{I}(U))(i))$, then the remainder maps the polynomial $X^i h(T)$ to $Y^{q^2-1-i}(T^i h(T) \mod T^q + T - 1)$. But the definition of R implies that mapping $h(T)$ to $T^i h(T) \mod T^q + T - 1$ is given by $\mathbf{h} \mapsto \mathbf{h}R_i$, where $\mathbf{h} = (h_0, h_1, \ldots, h_{q-1})$ is the coefficient vector of $h(T)$. □

To find the dimension of $(\Gamma_2, RS(\mathfrak{I},k) : RS(\mathfrak{I},k))$ we need to find the elements of $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_1(k))$ whose remainders belong to $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_2(k))$. Because the remainder induces a bijection between $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_1}(\mathbf{I}(U))(i))$ and $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_2}(\mathbf{I}(U))(q^2-1-i))$ we can divide the work by finding elements of $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_1(k) \cap \Delta_{\preceq_1}(\mathbf{I}(U))(i))$ whose remainders belong to the linear space $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_2(k) \cap \Delta_{\preceq_2}(\mathbf{I}(U))(q^2-1-i))$ for each i. For this purpose we will need the left nullspace of a $k \times (q-k)$ submatrix of the R_i matrices.

Definition 5.2.15 *Let $R_{i,k}$ denote the $k \times (q-k)$ submatrix of R obtained by taking the rows $i, i+1, \ldots, i+k-1$, the rows are indexed $\mod (q^2-1)$ and the last $q-k$ columns.*

The matrix $R_{i,k}$ represents the polynomials in $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_1(k) \cap \Delta_{\preceq_1}(\mathbf{I}(U))(i))$ which can be written as polyomials in $Span_{\mathbf{F}_{q^2}}(\Delta_{\preceq_1}(\mathbf{I}(U))(q^2-1-i))$ of degree k or more in T. The left corank of $R_{i,k}$ is equal to the dimension of the functions in $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_1(k) \cap \Delta_{\preceq_1}(\mathbf{I}(U))(i))$ whose remainders are in the $\mathbf{F}_{q^2}$-linear space $Span_{\mathbf{F}_{q^2}}(\mathcal{M}_2(k) \cap \Delta_{\preceq_2}(\mathbf{I}(U))(q^2-1-i))$.

The following lemma allows us to halve the number of submatrices we need to consider.

Lemma 5.2.16 *The rank of $R_{i,k}$ is equal to the rank of $R_{q^2-1-i,k}$.*

Proof.

The left nullspace of $R_{i,k}$ represents the space of solutions (f_1, f_2) to the equation $f_1(t)t^i = f_2(t) \mod t^q + t - 1$ where the degree of f_1 and f_2 is less than k. Since t^i is invertible, we may multiply both sides by t^{q^2-1-i} to obtain a solution of the form (f_2, f_1) to the equation $f_1(t) = f_2(t)t^{q^2-1-i} \mod t^q + t - 1$. These solutions are represented by the left nullspace of $R_{q^2-1-i,k}$. □

Theorem 5.2.17 *If $1 \le k \le \frac{q}{2}$, then $(\Gamma_2, RS(\mathfrak{I},k) : RS(\mathfrak{I},k))$ has dimension at least k^3. If $\frac{q}{2} \le k \le q$, then $(\Gamma_2, RS(\mathfrak{I},k) : RS(\mathfrak{I},k))$ has dimension at least $(q^2-1)(2k-q) + (q-k)^3$.*

Proof.

Let $i = i_1 q + i_0$ where $0 \le i_1 + i_0 \le k-1 < \frac{q}{2}$. Let $j \ge k$, then $j - i_0, i_1 \le k - i_0$. Therefore the binomial coefficient is equal to $(-1)^{j-i_0}\binom{i_1}{j-i_0} = 0$. On the other

hand this is equal to the entry $r_{i,j}$ of the matrix R. Therefore, in the case $i = i_1 q + i_0$, where $0 \leq i_1 + i_0 \leq k - 1 < \frac{q}{2}$, the matrix $R_{i,k}$ has at least $k - i_0 - i_1$ zero rows. The left nullspace of $R_{i,k}$ has rank k. For $i = 1, 2, \ldots k-1$, the left nullspace of $R_{i,k}$ is at least $k - i$. For $i_1 < k$, the matrix $R_{i_1 q,k}$ has its first $k - i_1$ rows equal to 0. Therefore, for $i_0 < k - i_1$ the left nullspace of $R_{i_1 q + i_0,k}$ is at least $k - i_1$. However, this also holds for $R_{i_1 q - i_0,k}$. Now we can count the total left nullity to obtain that left corank of all matrices is at least $k + 2\binom{k}{2} + 2\sum_{i=1}^{k-1}(2\binom{k-i}{2} + (k-i)(i+1))$. This is equal to k^3. Corollary 3.2.11 implies the second statement of the theorem. □

Like in the previous section we will prove equality for $q = 2^h$ and $q = p$. As in the previous section we will use the matrix of binomial coefficients $B(k, h, r)$. However since the entries of R alternate in sign we need some preliminary theorems.

Definition 5.2.18 *Let k, h, r be integers. We define*

$$B'(k, h, r) := \left((-1)^{-v+u} \binom{k}{r + h - v + u} \right)_{0 \leq u, v \leq h}.$$

Theorem 5.2.19 *The matrices $B(k, h, r)$ and $B'(k, h, r)$ have the same rank.*

Proof.

The matrix $B'(k, h, r)$ is obtained by multiplying every second row and every second column of the matrix $B(k, h, r)$ by -1. □

Theorem 5.2.20 *Let q be a power of 2 or a prime. If $1 \leq k \leq \frac{q}{2}$, then the code $(\Gamma_2, RS(\mathfrak{I}, k) : RS(\mathfrak{I}, k))$ has dimension k^3. If $\frac{q}{2} \leq k \leq q$, then $(\Gamma_2, RS(\mathfrak{I}, k) : RS(\mathfrak{I}, k))$ has dimension $(q^2 - 1)(2k - q) + (q - k)^3$.*

Proof.

We will prove that all nonzero rows of $R_{i,k}$ are independent, which makes the bound in Theorem 5.2.17 sharp. The technique we will use is similar to the techniques in Lemmas 5.1.21 and 5.1.22.

Let $i = i_1 q + i_0, 0 \leq i_0 \leq q - k$. In this case, the first $k - i_1 - 1$ rows of $R_{(i_1+1)q+i_0,k}$ are $\mathbf{0}$. The other $i_1 + 1$ rows contain $B'(i_1, i_0, i_1)$ as the submatrix corresponding to the first k columns of $R_{(i_1+1)q+i_0,k}$. From [Mat08] we know this submatrix has full rank.

Since the first $k-i_1-1$ rows of $R_{(i_1+1)q,k}$ are 0, the matrix $B'(i_1,i_0,i_1)$ is also a full rank submatrix of $R_{(i_1+1)q+i_0,k}$ where $0 \leq i_0 \leq q-(i_1+1)$.

Finally, we consider the case $i_1q \leq i_1q+i_0 \leq (i_1+1)q$, where $(i_1+1) \leq k \leq \frac{q}{2}$ and $i_0 \geq q-i_1$. The matrix $R_{i_1q+i_0,k}$ has $q-i_0$ rows with binomial coefficients $(-1)^j\binom{i_1}{j}$ and $k+i_0-q$ rows with binomial coefficients $(-1)^j\binom{i_1+1}{j}$. The columns of $\mathbf{R}$ corresponding to the nonzero binomial coefficients $(-1)^j\binom{i_1+1}{j}$ are the columns from k to i_0 and the columns corresponding to the nonzero binomial coefficients $(-1)^j\binom{i_1}{j}$ are the columns from i_1+1 to $q-1$. Therefore, $R_{i_1q+i_0,k}$ has $B'(i_1+1,i_0,i_0-k)$ as a submatrix on the first columns and $B'(i_1,q-i_0,q-i_1)$ on the last. Therefore, $R_{i_1q+i_0,k}$ has full rank.

The rank for the matrices $R_{i,k}$ where i has not been determined so far follows from the fact that $R_{i,k}$ and $R_{q^2-1-i,k}$ have the same rank. This proves the theorem from $1 \leq k \leq \frac{q}{2}$. Corollary 3.2.11 implies the theorem is true for $\frac{q}{2}$. □

5.2.1 Parameters of $(\Gamma_2, RS(\mathfrak{I},k) : RS(\mathfrak{I},k))$

We use the following theorem from [HJ11] and [RS06] to estimate the minimum distance of the graph codes $(\Gamma_2, RS(\mathfrak{I},k) : RS(\mathfrak{I},k))$.

Theorem 5.2.21 *The minimum distance of* $(\Gamma_2, RS(\mathfrak{I},k) : RS(\mathfrak{I},k))$*, denoted by* D*, satisfies the following:*

- $D \geq (q-k+1)((q-k+1)^2-(q-k))$.
- $D \geq (q^2-1)(q-k+1)\frac{q-k+1-\sqrt{q}}{q-\sqrt{q}}$.

For the case $q=4$ and $k=2$, the bounds on the minimum distance are $D \geq 3^2+(3^2-2)=16$ and $D \geq 15*3*\frac{1}{2}=23$. A direct computation shows $D=31$. In this case, we can obtain an improvement from the derived footprint bound as given in [Gei08]. From the monomials of the form X^iT^j which generate $(\Gamma_2, RS(\mathfrak{I},2) : RS(\mathfrak{I},2))$ we obtain $D \geq 28$. A direct computation shows this is a $[60,8,31]_{\mathbf{F}_4}$ code.

As in the previous section for the graph code $(\Gamma_2, RS(\mathfrak{I},3) : RS(\mathfrak{I},3))$ we have the graph code bound $D \geq 6$. This bound is sharp since the code is a $[60,29,6]_{\mathbf{F}_4}$ code. The bound in [Gei08] gives $D \geq 4$.

5.3 Iterative encoding

A forcing set is a subset S of the edges of a graph G with the property that any codeword of any graph code $(G, C_1 : C_2)$, with C_1 and C_2 as MDS codes, is determined by the values at the positions in S. In particular S is independent of the endpoint labeling functions.

Definition 5.3.1 *Let G an (n_1, n_2)-regular graph. Let $k_1 \leq n_1$ and $k_2 \leq n_2$. Let $T \subseteq E(G)$. We say T is* (k_1, k_2)-closed *if T satisfies:*

$$\forall v \in V_1(G)\ \#(T \cap E(u)) \geq k_1 \rightarrow E(v) \subseteq T,$$
$$\forall u \in V_2(G)\ \#(T \cap E(u)) \geq k_2 \rightarrow E(u) \subseteq T.$$

That is if there are at least k_1 edges incident to $v \in V_1(G)$ contained in T, then the whole of $E(v)$ is contained in T. Also holds similarly for $u \in V_2(G)$.

To find a (k_1, k_2)closed set which contains a subset of edges, say $S \subset E(G)$ one can check all vertices to see if they have k_1 (or k_2) incident edges in S. Then one defines S_1 as the set of edges in S plus those edges incident to a vertex with k_1 (or k_2) incident edges in S. Then one does the same with S_1 to get an S_2 and so on. This process terminates, and the final result is a (k_1, k_2) closed set containing S. In fact we prove that by doing this, we get the smallest closed set containing S. The sets S_i in the proof are constructed by adding one set of incident edges at a time, but this makes no difference.

Theorem 5.3.2 *Let G an (n_1, n_2)-regular graph. Let $k_1 \leq n_1$ and $k_2 \leq n_2$. Let $S \subseteq E(G)$. There exists a unique smallest (k_1, k_2)-closed set containing S.*

Proof.

We define Z as follows $Z = S \cup E(z_1) \cup E(z_2) \cup \ldots \cup E(z_a)$, where the subset Z satifies:

- $Z_0 = S$.
- $Z_i := S \cup E(z_1) \cup E(z_2) \cup \ldots \cup E(z_i)$ satisfies $Z_i \cap E(z_{i+1}) \geq k_1$ or $Z_i \cap E(z_{i+1}) \geq k_2$ depending on $z_{i+1} \in V_1(G)$ or $z_{i+1} \in V_2(G)$.
- Z is (k_1, k_2)-closed.

We claim that if Z' is another (k_1, k_2)-closed containing S then it must also contain Z. Suppose Z' is (k_1, k_2)-closed and Z contains S. Now suppose $Z \not\subseteq Z'$ then there exists Z_i such that $Z_i \subseteq Z'$ but $Z_{i+1} \not\subseteq Z'$, but since $Z_i \cap E(z_{i+1}) \geq k_1$ or $Z_i \cap E(z_{i+1}) \geq k_2$ depending on $z_{i+1} \in V_1(G)$ or $z_{i+1} \in V_2(G)$ it follows that $Z_{i+1} \subseteq Z'$. Therefore, $Z \subseteq Z'$. □

Definition 5.3.3 *Let G an (n_1, n_2)-regular graph. Let k_1, k_2 be integers satisfying $k_1 \leq n_1$ and $k_2 \leq n_2$. Let $S \subseteq E(G)$. We define the unique smallest (k_1, k_2)-closed set containing S as the* (k_1, k_2)-closure of S. *We denote it by $cl_{k_1,k_2}(S)$. If $cl_{k_1,k_2}(S) = E(G)$ we say S is an* (k_1, k_2) forcing set.

The following theorem relates the size of a (k_1, k_2) forcing set of G with the dimension of a graph code with $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ MDS component codes.

Theorem 5.3.4 *Suppose G is an (n_1, n_2) regular bipartite graph. Let C_1 be an MDS code of length n_1 and dimension k_1 and let C_2 be an MDS code of length n_2 and dimension k_2. Let S be a (k_1, k_2) forcing set of G. Then $(G, C_1 : C_2)$ is linearly isomorphic to $(G, C_1 : C_2)^S$ and* $\dim(G, C_1 : C_2) \leq \#S$.

Proof.

Consider $(G, C_1 : C_2)^S$, the projection of $(G, C_1 : C_2)$ onto S. There is a linear map from $(G, C_1 : C_2)$ to $(G, C_1 : C_2)^S$ where we map the codeword $c = (c_i)_{i \in E(G)}$ to the vector $c_S = (c_i)_{i \in S}$. We will prove the kernel is zero dimensional. Let c be a codeword of $(G, C_1 : C_2)$ which is mapped to the zero codeword of $(G, C_1 : C_2)^S$. Therefore, $c_i = 0$ for $i \in S$. For each $v \in V_1(G)$ once we know $c_i = 0$ for k_1 edges of $E(v)$, we know $c_i = 0$ for all edges of $E(v)$. For each $u \in V_2(G)$ once we know $c_i = 0$ for k_2 edges of $E(u)$ are zero, we know $c_i = 0$ for all edges of $E(u)$. Therefore the set of zero positions of the codeword c is $cl_{k_1,k_2}(S)$. Since S is a (k_1, k_2) forcing set of G all positions of c have the entry zero.

Since the linear map $(G, C_1 : C_2)$ to $(G, C_1 : C_2)^S$ has a trivial kernel, puncturing $(G, C_1 : C_2)$ on S is a linear isomorphism between $(G, C_1 : C_2)$ and $(G, C_1 : C_2)^S$. Therefore, the dimension of $(G, C_1 : C_2)$ is equal to the dimension of $(G, C_1 : C_2)^S$ which is at most $\#S$. □

The hypothesis that the component codes are MDS can't be relaxed. In this case, one can find graph codes where the dimension of the graph code is larger

than the size of the forcing set. For example:

Example 5.3.5 *Let G be the 4-cycle. Any single edge of G constitutes a $(1,1)$ forcing set. We use the following endpoint labelings for a graph code over G: the edges $(1,2)$ and $(3,4)$ get label 1 for both endpoints and the edges $(2,3)$ and $(1,4)$ get label 2 for both endpoints. This is an endpoint labeling of the cycle. Let $C = Span((1,\alpha))$, the graph code $(G, C : C)$ is the code $Span((1,\alpha,1,\alpha))$. But if we let $C' = Span((1,0))$. The graph code $(G, C' : C')$ is the code $Span(\{(1,0,0,0),(0,0,1,0)\})$.*

We also get a corollary to Theorem 5.3.4. We may encode $(G, C_1 : C_2)$ iteratively from a codeword in $(G, C_1 : C_2)^S$ where S is a (k_1, k_2) forcing set of G and C_1 and C_2 are MDS codes of dimensions k_1 and k_2 respectively. Once some positions of the codeword in $(G, C_1 : C_2)^S$ have been determined, it might be possible to determine the positions of some other neighborghood which has at least k_2 but not n_2 positions determined. The other possibility is that it might not be possible to extend the entries of the code in this way, but we will prove this is not the case.

Theorem 5.3.6 *Suppose G is an (n_1, n_2) regular bipartite endpoint labeled graph. Let C_1 be an MDS code of length n_1 and dimension k_1 and C_2 an MDS code of length n_2 and dimension k_2. Let S be a (k_1, k_2) forcing set of G. Then a codeword $c' \in (G, C_1 : C_2)^S$ may be extended uniquely to a codeword in $(G, C_1 : C_2)$ using only the conditions that $(G, C_1 : C_2)^{E(v)} \equiv C_1$, for $v \in V_1(G)$ and $(G, C_1 : C_2)^{E(v)} \equiv C_2$, for $u \in V_2(G)$.*

Proof.

Let S be a (k_1, k_2) forcing set. There exist $S_0, S_1, \ldots, S_m \subseteq E(G)$ satisfying: $S_0 = S$, $S_m = E(G)$ and for $i = 1, 2, \ldots n$ either the set $S_i = S_{i-1} \cup E(u_i)$ where $k_1 \leq \#(S_{i-1} \cup E(v_i)) < n_1$ and $v_i \in V_1(G)$ or the set $S_i = S_{i-1} \cup E(u_i)$ where $k_2 \leq \#(S_{i-1} \cup E(u_i)) < n_2$ and $u_i \in V_2(G)$.

Let ϕ_{S_i} denote the linear map from $(G, C_1 : C_2)$ to $(G, C_1 : C_2)^{S_i}$. Since S_i is a (k_1, k_2) forcing set of G then ϕ_{S_i} is a linear isomorphism.

Let $\phi_S(c) = c' \in (G, C_1 : C_2)^S = (G, C_1 : C_2)^{S_0}$. Now suppose that we have extended c' to $\phi_{S_i}(c) \in (G, C_1 : C_2)^{S_i}$ and we want to prove that we can extend it uniquely to a codeword of $(G, C_1 : C_2)^{S_{i+1}}$. The only possibility is to extend $\phi_{S_i}(c)$ to $\phi_{S_{i+1}}(c)$ because the positions in $S_{i+1} \backslash S_i$ are determined by the entries in $\phi_{S_i}(c)$ and those positions are exactly the entries of $\phi_{S_{i+1}}(c)$. □

5.4 Twisted Γ_1

Now we assume q is a square prime power and $r = \sqrt{q}$. We define a graph Γ_t which is closely related to Γ_1.

Definition 5.4.1 *We define the graph Γ_t as the following bipartite graph. The vertex set $V_1(\Gamma_t) := V_1(\Gamma_1) = \{(x, y) \in \mathbf{F}_q \times \mathbf{F}_q\}$. Likewise the vertex set $V_2(\Gamma_t) := V_2(\Gamma_1) = \{(a, b) \in \mathbf{F}_q \times \mathbf{F}_q\}$.*

We define $E(\Gamma_t) := \{((x, y), (a, b)) \in V_1(\Gamma_t) \times V_2(\Gamma_t) \mid a^r x + b^r - y = 0\}$.

Note that Γ_t is also (q, q) regular bipartite graph on the same vertices as Γ_1. In fact both graphs are isomorphic. The only difference is that the incidence relation $ax + b - y$ is twisted with the field involution to obtain the relation $a^r x + b^r - y = 0$, and since we are working within $\mathbf{F}_q$ we also obtain another relation $ax^r + b - y^r = 0$. This twist changes significantly the graph codes $(\Gamma_t, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ under the following endpoint labeling.

Definition 5.4.2 *We use the following bijections to make a (q, q)-regular endpoint labeled bipartite graph with Γ_t.*

$$\forall (a, b) \in V_2(\Gamma_t), \phi_{(a,b)} : \mathbf{F}_q \to E((a, b))$$
$$\phi_{(a,b)}(x) = (x, a^r x + b^r, a, b)$$
$$\forall (x, y) \in V_1(\Gamma_t), \chi_{(x,y)} : \mathbf{F}_q \to E((x, y))$$
$$\chi_{(x,y)}(a) = (x, y, a, y^r - ax^r)$$

We have found the following dimensions of $(\Gamma_t, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ and (k, k) forcing sets of the following sizes:

$q = 4$

k	K	$\#S$
1	1	1
2	10	10
3	33	33
4	64	64

$q = 16$

k	K	$\$S$
1	1	1
2	9	9
3	36	37
4	101	103
5	208	211
6	357	361
7	549	554
8	784	790
9	1061	1068
10	1381	1389
11	1744	1751
12	2149	2156
13	2596	2600
14	3081	3081
15	3585	3585
16	4096	4096

$q = 9$

k	K	$\#S$
1	1	1
2	9	9
3	37	37
4	91	91
5	172	172
6	280	280
7	414	414
8	568	568
9	729	729

T. Høholdt and J. Justesen proved that for $r \leq k \leq q - r$ the dimension of $(\Gamma_t, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ in the cases where $k = 2r - 1, 3r - 2, \ldots q - r + 1$ is $q^2 k \frac{k-r}{q-r} + \binom{r+1}{2}^2 + 1$ with techniques shown in this chapter. It seems the dimension of the graph code $(\Gamma_t, RS(\mathbf{F}_q, k) : RS(\mathbf{F}_q, k))$ is optimal or almost so. However, a proof has eluded us so far.

Chapter 6

Affine Grassmann and Grassmann Codes

The Grassmannian is a mathematical object relevant in Algebra, Geometry and Combinatorics. In this chapter, we define the Grassmannian, Grassmann codes and affine Grassmann codes. We also define some graphs such that Grassmann codes and affine Grassmann codes are Tanner codes over these graphs in a natural, nontrivial way.

6.1 Minimum weight Codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$

The codes $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ were introduced in chapter 2 as an example of an evaluation code. We repeat their definition for the benefit of the reader. In this chapter we define $m := \ell + \ell'$.

Definition 6.1.1 *Let $\boldsymbol{M}$ be an $\ell \times \ell'$ matrix, where $\ell \leq \ell'$. Suppose I is a subset of $\{1, 2, \ldots, \ell\}$ and $J \subseteq \{1, 2, \ldots, \ell'\}$. Suppose $\#I = \#J = h \leq r$. Let $M_{I,J}$ denote the submatrix of M obtained by taking the rows specified by I and the columns specified by J. An h-minor of $\boldsymbol{M}$ is the determinant of an $h \times h$ submatrix of $\boldsymbol{M}$. The minor determined by I and J is denoted by $det(\boldsymbol{M}_{I,J})$. When $h = \ell$ we omit I from the notation. The 0-minor is defined as 1.*

Consider the set of $\ell \times \ell'$ matrices over $\mathbf{F}_q$, $\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$. We identify $\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$ with the set of points of the affine space $\mathbb{A}(\ell\ell', \mathbf{F}_q)$. We associate to this affine space the polynomial ring $\mathbf{F}_q[\mathbf{X}]$. The polynomial ring is defined in the $\ell\ell'$ indeterminates of the matrix $\mathbf{X} := (X_{i,j})_{1\leq i\leq \ell, 1\leq j\leq \ell'}$.

Definition 6.1.2 *Let $\boldsymbol{X} := (X_{i,j})_{1\leq i\leq \ell, 1\leq j\leq \ell'}$ be an $\ell \times \ell'$ matrix in the indeterminates $X_{i,j}$. For $0 \leq h \leq \ell$ we denote $\omega_h(\boldsymbol{X})$ as the set of all h-minors of X. We define the* affine Grassmann code, *$\mathcal{C}^{\mathbb{A}}(\ell, m)$, as the affine variety code $C(\mathbf{F}_q[\boldsymbol{X}], Span_{\mathbf{F}_q}(\omega_0(\boldsymbol{X}) \cup \omega_1(\boldsymbol{X}) \cup \ldots \cup \omega_h(\boldsymbol{X})))$.*

From [BGH12] we know that $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ is generated by its minimum weight codewords. Additionally, over $\mathbf{F}_2$ the minimum distance $d(\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp})$ is 4. Over other fields, $d(\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp})$ is 3. Now we study the minimum distance codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$. First we need the following lemma about the automorphisms of $\mathcal{C}^{\mathbb{A}}(\ell, m)$. We denote the group of nonsingular $\ell\times\ell$ matrices over $\mathbf{F}_q$ by $\mathbf{GL}_\ell(\mathbf{F}_q)$.

Lemma 6.1.3 *[BGH12] Suppose $\boldsymbol{B} \in \mathbf{GL}_\ell(\mathbf{F}_q)$, $\boldsymbol{A} \in \mathbf{GL}_{\ell'}(\mathbf{F}_q)$ and the matrix $\boldsymbol{U} \in \mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$. Suppose $f \in Span_{\mathbf{F}_q}(\omega_0(\boldsymbol{X}) \cup \omega_1(\boldsymbol{X}) \cup \ldots \cup \omega_h(\boldsymbol{X}))$. Then, the map $\boldsymbol{M} \mapsto \boldsymbol{BMA} + \boldsymbol{U}$ where $\boldsymbol{M} \in \mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$ induces an automorphism of $\mathcal{C}^{\mathbb{A}}(\ell, m)$ which is the map*

$$ev_{\mathbf{F}_q[\boldsymbol{X}]}(f(\boldsymbol{X})) \mapsto ev_{\mathbf{F}_q[\boldsymbol{X}]}(f(\boldsymbol{BXA} + \boldsymbol{U})).$$

We denote the map $\mathbf{M} \mapsto \mathbf{BMA} + \mathbf{U}$ by $\sigma_{\mathbf{B},\mathbf{A},\mathbf{U}}$. The group of such maps is denoted by $\mathfrak{H}(\ell, m)$. We also look at two subgroups of $\mathfrak{H}(\ell, m)$, the group of matrix products, $\sigma_{\mathbf{B},\mathbf{A},\mathbf{0}}$ and the group of matrix translations $\sigma_{\mathbf{I}_\ell,\mathbf{I}_{\ell'},\mathbf{U}}$. The full automorphism group is determined in [GK13], but for us $\mathfrak{H}(\ell, m)$ suffices.

Definition 6.1.4 *Let $\boldsymbol{E}_{i,j}$ denote the $\ell \times \ell'$ matrix whose (i, j)–th entry is* 1 *and all other entries are* 0 *and $\boldsymbol{D}_\rho := \boldsymbol{E}_{1,1} + \boldsymbol{E}_{2,2} + \cdots \boldsymbol{E}_{\rho,\rho}$.*

Lemma 6.1.5 *Let $\boldsymbol{M}$ be an $\ell\times\ell'$ matrix of rank ρ. Then there exists matrices $\boldsymbol{B} \in \mathbf{GL}_\ell(\mathbf{F}_q)$, $\boldsymbol{A} \in \mathbf{GL}_{\ell'}(\mathbf{F}_q)$ such that $\sigma_{\boldsymbol{B},\boldsymbol{A},\boldsymbol{0}}(\boldsymbol{M}) = \boldsymbol{D}_\rho$.*

6.1.1 Affine Grassmann codes over $\mathbf{F}_q, q \neq 2$

Now we consider the case where $q \neq 2$. Over nonbinary fields the weight 3 codewords generate $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$. We characterize all minimum weight codewords. From this characterization we can count the minimum weight codewords geometrically and consider the affine Grassmann codes as a Tanner code from the minimum weight codewords.

THEOREM 6.1.6 *Let c be a codeword of weight 3 of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ where $supp(c)$ equals $\{\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3\}$ and $c_{\boldsymbol{N}_1} = 1$, $c_{\boldsymbol{N}_2} = a \neq 0$, and $c_{\boldsymbol{N}_3} \neq 0$. There exists a translation in $\mathfrak{H}(\ell, m)$ such that the image of c under this translation, the codeword c', satisfies $supp(c') = \{\boldsymbol{0}, \boldsymbol{D}_1, \frac{a}{a+1}\boldsymbol{D}_1\}$ and the nonzero coefficients of c' are $c'_{\boldsymbol{0}} = 1$, $c'_{\boldsymbol{D}_1} = a$, $c'_{\frac{a}{a+1}\boldsymbol{D}_1} = c_{\boldsymbol{N}_3} = -(a+1)$.*

PROOF.

Suppose c satisfies the hypothesis of the theorem. We let c' be the image of c under $\sigma_{\mathbf{I}_\ell, \mathbf{I}_{\ell'}, -\mathbf{N}_1}$. Therefore $supp(c')$ is $\{\mathbf{0}, \mathbf{N}_2 - \mathbf{N}_1, \mathbf{N}_3 - \mathbf{N}_1\}$. To simplify the notation we let $\mathbf{M} = \mathbf{N}_2 - \mathbf{N}_1$ and $\mathbf{N} = \mathbf{N}_3 - \mathbf{N}_1$. The nonzero coefficients of c' are $c'_{\mathbf{0}} = 1$, $c'_{\mathbf{M}} = a$ and $c'_{\mathbf{N}} = c_{\mathbf{N}_3} \neq 0$. Now we examine the conditions given by $c \cdot d = 0$ for $d \in \mathcal{C}^{\mathbb{A}}(\ell, m)$.

First, let d be $(1, 1, \ldots, 1)$. The condition $c \cdot d = 0$ is $c'_{\mathbf{0}} + c'_{\mathbf{M}} + c'_{\mathbf{N}} = 0$. Therefore, $c'_{\mathbf{N}} = -(a+1) \neq 0$ and $a \neq -1$.

Now let $f = det(\mathbf{X}_{\{i\},\{i\}})$ and let $d = ev_{\mathbf{F}_q[\mathbf{X}]}(f(\mathbf{X}))$ In this case, the condition $c \cdot d = 0$ is equivalent to $a\mathbf{M}_{i,j} - (a+1)\mathbf{N}_{i,j} = 0$. This implies $\mathbf{N}_{i,j} = \frac{a}{a+1}\mathbf{M}_{i,j}$. Therefore, $\mathbf{N}$ equals $\frac{a}{a+1}\mathbf{M}$.

To finish the proof, let $f = det(\mathbf{X}_{I,J})$ where f is a 2-minor. Let d be the codeword corresponding to the evaluation of f. The condition $c \cdot d = 0$ is equivalent to $af(\mathbf{M}) - (a+1)f(\mathbf{N}) = 0$. But $\mathbf{N} = \frac{a}{a+1}\mathbf{M}$. Therefore, we rewrite $c \cdot d = 0$ as $af(\mathbf{M}) - (a+1)f(\frac{a}{a+1}\mathbf{M}) = 0$, which implies, $f(\frac{a}{a+1}\mathbf{M}) = (\frac{a}{a+1})^2 f(\mathbf{M})$. The original equation is now $af(\mathbf{M}) - (a+1)(\frac{a}{a+1})^2 f(\mathbf{M}) = 0$. We can eliminate a as a common factor in both terms and reduce the equation to $f(\mathbf{M}) - (\frac{a}{a+1})f(\mathbf{M}) = 0$. But this is equal to $\frac{1}{a+1}f(\mathbf{M}) = 0$. Since $\frac{1}{a+1} \neq 0$, then $f(\mathbf{M}) = 0$. Since all 2-minors of $\mathbf{M}$ vanish then $\mathbf{M}$ has rank 1. Lemma 6.1.5 implies there exists $\sigma_{\mathbf{B},\mathbf{A},\mathbf{0}} \in \mathfrak{H}(\ell, m)$ such that $\sigma_{\mathbf{B},\mathbf{A},\mathbf{0}}(\mathbf{M}) = \mathbf{D}_1$. □

THEOREM 6.1.7 *There are*

$$\frac{q^{\ell\ell'}(q-2)(q^{\ell}-1)(q^{\ell'}-1)}{3!}$$

codewords of weight 3 in $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$.

PROOF.

Theorem 6.1.6 implies that the support minimum weight codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ is a subset of 3 elements of a set of the form $Span_{\mathbf{F}_q}(\mathbf{M}) + \mathbf{U}$, where $\mathbf{M}$ is a

matrix of rank 1.

There are $\frac{(q^\ell-1)(q^{\ell'}-1)}{(q-1)^2}$ sets of the form $Span_{\mathbf{F}_q}(\mathbf{M})$, where $\mathbf{M}$ is a matrix of rank 1. For each linear subspace of matrices, there are $q^{\ell\ell'-1}$ possible translates $Span_{\mathbf{F}_q}(\mathbf{M})+\mathbf{U}$. At each translate there are $\binom{q}{3}$ supports of a minimum weight codeword, and for each support there are $q-1$ minimum weight codewords. □

Note that this formula also works for the number of weight 3 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ over $\mathbf{F}_2$. That is the formula evaluates to 0 for $q=2$.

6.1.2 Dual Affine Grassmann codes over $\mathbf{F}_2$

Using the automorphisms in $\mathfrak{H}(\ell,m)$ we can look at the codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ of weight 4. If the support of $c\in\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ is the set $\{\mathbf{M}_1,\mathbf{M}_2,\mathbf{M}_3,\mathbf{M}_4\}$. then for any h-minor f, $f(\mathbf{M}_1)+f(\mathbf{M}_2)+f(\mathbf{M}_3)+f(\mathbf{M}_4)=0$. We study the restrictions imposed on the pairwise distinct matrices $\mathbf{M}_1,\mathbf{M}_2,\mathbf{M}_3,\mathbf{M}_4$.

Lemma 6.1.8 *Let $c\in\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ such that $supp(c)=\{\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3,\boldsymbol{M}_4\}$ then, there exists a codeword $c'\in\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ such that its support set $supp(c')$ is $\{\boldsymbol{0},\boldsymbol{M}_1+\boldsymbol{M}_4,\boldsymbol{M}_2+\boldsymbol{M}_4,\boldsymbol{M}_3+\boldsymbol{M}_4\}$.*

Proof. Take c' as the image of c under the automorphism $\sigma_{\mathbf{I}_\ell,\mathbf{I}_{\ell'},\mathbf{M}_4}$. □

Now we will look at the conditions given by $f(\mathbf{0})+f(\mathbf{M}_1)+f(\mathbf{M}_2)+f(\mathbf{M}_3)=0$.

Lemma 6.1.9 *Let $c\in\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$. Suppose $supp(c)=\{\boldsymbol{0},\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3\}$ then,*

$$\boldsymbol{M}_1+\boldsymbol{M}_2=\boldsymbol{M}_3.$$

Proof.

Let $f=det(\mathbf{X}_{\{i\},\{j\}})$. Since $f(\mathbf{0})+f(\mathbf{M}_1)+f(\mathbf{M}_2)+f(\mathbf{M}_3)=0$ we have that $(\mathbf{M}_1)_{i,j}+(\mathbf{M}_2)_{i,j}=(\mathbf{M}_3)_{i,j}$. This implies $\mathbf{M}_1+\mathbf{M}_2=\mathbf{M}_3$. □

Lemma 6.1.10 *Let $c\in\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$. Suppose $supp(c)=\{\boldsymbol{0},\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_1+\boldsymbol{M}_2\}$. If the rank of $\boldsymbol{M}_1$ is ρ then there exists a codeword $c'\in\mathcal{C}^{\mathbb{A}}(\ell,m)^\perp$ such that its support $supp(c')$ is $\{\boldsymbol{0},\boldsymbol{D}_\rho,\boldsymbol{M},\boldsymbol{D}_\rho+\boldsymbol{M}\}$.*

PROOF. This is a direct consequence of Lemma 6.1.5. □

Now we look at the restrictions the 2-minors impose on ρ and $\mathbf{M}$ when we have a codeword $c \in \mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ whose support is $\{\mathbf{0}, \mathbf{D}_\rho, \mathbf{M}, \mathbf{D}_\rho + \mathbf{M}\}$. Over $\mathbf{F}_2$ the $(1,1)$-th entry of either $\mathbf{M}$ or $\mathbf{D}_\rho + \mathbf{M}$ is zero, thus without loss of generality we assume for the remainder of this section that $(\mathbf{M})_{1,1} = 0$.

LEMMA 6.1.11 *Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ such that $supp(c) = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}$. Then $\boldsymbol{M}_{i,i} = 0$.*

PROOF.

Note that by hypothesis $(\mathbf{M}_{1,1}) = 0$. First, we consider $f = det(\mathbf{X}_{\{1,i\},\{1,i\}})$ where $1 < i \leq \rho$. In this case,

$$f(\mathbf{0}) = 0, f(\mathbf{D}_\rho) = 1, f(\mathbf{M}) = \mathbf{M}_{1,i}\mathbf{M}_{i,1}, f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,i} + 1 + \mathbf{M}_{1,i}\mathbf{M}_{i,1}.$$

The condition $f(\mathbf{0}) + f(\mathbf{D}_\rho) + f(\mathbf{M}) + f(\mathbf{M} + \mathbf{D}_\rho) = 0$ implies $\mathbf{M}_{i,i} = 0$.

Now, we consider the 2-minor $f = det(\mathbf{X}_{\{1,i\},\{1,i\}})$ where $i > \rho$. In this case,

$$f(\mathbf{0}) = 0, f(\mathbf{D}_\rho) = 0, f(\mathbf{M}) = \mathbf{M}_{1,i}\mathbf{M}_{i,1}, f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,i} + \mathbf{M}_{1,i}\mathbf{M}_{i,1}.$$

The condition $f(\mathbf{0}) + f(\mathbf{D}_\rho) + f(\mathbf{M}) + f(\mathbf{M} + \mathbf{D}_\rho) = 0$ implies $\mathbf{M}_{i,i} = 0$. □

LEMMA 6.1.12 *Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ such that $supp(c) = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}$. Suppose both $i, j > 1$ and $i > \rho$ or $j > \rho$, then $\boldsymbol{M}_{i,j} = 0$.*

PROOF.

We consider the 2-minor $f = det(\mathbf{X}_{\{1,i\},\{1,j\}})$ where $i > \rho$ or $j > \rho$. In this case,

$$f(\mathbf{0}) = 0, f(\mathbf{D}_\rho) = 0, f(\mathbf{M}) = \mathbf{M}_{1,j}\mathbf{M}_{i,1}, f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,j} + \mathbf{M}_{1,j}\mathbf{M}_{i,1}.$$

The condition $f(\mathbf{0}) + f(\mathbf{D}_\rho) + f(\mathbf{M}) + f(\mathbf{M} + \mathbf{D}_\rho) = 0$ implies $\mathbf{M}_{i,j} = 0$. □

We have now proven that there is a codeword in $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ with support in $\{\mathbf{0}, \mathbf{D}_\rho, \mathbf{M}, \mathbf{D}_\rho + \mathbf{M}\}$ then the entries of the four matrices is 0 outside of the $\rho \times \rho$ submatrix given by $\mathbf{D}_\rho$. Now we prove that ρ has to be small.

Lemma 6.1.13 *Let $c \in \mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ such that supp$(c) = \{\boldsymbol{0}, \boldsymbol{D}_\rho, \boldsymbol{M}, \boldsymbol{D}_\rho + \boldsymbol{M}\}$. Then $\rho = 1$ or $\rho = 2$.*

Proof.

Since the matrices in the support of c are different, $\mathbf{D}_\rho \neq \mathbf{0}$, which implies $\rho > 0$. Now we will assume $\rho \geq 3$ and obtain a contradiction, namely $\mathbf{M} \neq \mathbf{0}$. We consider the 2-minor $f = det(\mathbf{X}_{\{1,i\},\{1,j\}})$ where $1 < i < j \leq \rho$ (Note that $1 < i < j \leq 2$ is impossible). In this case,

$$f(\mathbf{0}) = 0, f(\mathbf{D}_\rho) = 0, f(\mathbf{M}) = \mathbf{M}_{1,j}\mathbf{M}_{i,1}, f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{i,j} + \mathbf{M}_{1,j}\mathbf{M}_{i,1}.$$

The condition $f(\mathbf{0})+f(\mathbf{D}_\rho)+f(\mathbf{M})+f(\mathbf{M}+\mathbf{D}_\rho) = 0$ implies $\mathbf{M}_{i,j} = 0$. Similarly, we may prove $\mathbf{M}_{j,i} = 0$ where $1 < i < j \leq \rho$.

Now we have not determined the entries of $\mathbf{M}$ on the first row and first column, except $\mathbf{M}_{1,1}$.

Now consider the 2-minor $f = det(\mathbf{X}_{\{1,\rho\},\{i,\rho\}})$ where $1 < i < \rho$ (Note that $1 < i < 2$ is impossible). Note that Lemma 6.1.11 implies $\mathbf{M}_{\rho,\rho} = 0$. In this case,

$$f(\mathbf{0}) = 0, f(\mathbf{D}_\rho) = 0, f(\mathbf{M}) = \mathbf{M}_{1,\rho}\mathbf{M}_{i,\rho}, f(\mathbf{M} + \mathbf{D}_\rho) = \mathbf{M}_{1,i} + \mathbf{M}_{1,\rho}\mathbf{M}_{i,\rho}.$$

The condition $f(\mathbf{0})+f(\mathbf{D}_\rho)+f(\mathbf{M})+f(\mathbf{M}+\mathbf{D}_\rho) = 0$ implies $\mathbf{M}_{1,\rho} = 0$. Similarly we may prove $\mathbf{M}_{i,1} = 0$.

Therefore, if $\rho \geq 3$ then all the entries of $\mathbf{M}$ are 0, which is a contradiction. □

Now we classify the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$.

Theorem 6.1.14 *Let c be a codeword of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$. Suppose supp$(c)$ is equal to $\{\boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_3, \boldsymbol{M}_4\}$. There exists a permutation in the group $\mathfrak{H}(\ell, m)$ such that the image of supp(c) is one of the following:*

i) $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{E}_{1,2}, \boldsymbol{D}_1 + \boldsymbol{E}_{1,2}\}$,

ii) $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{E}_{2,1}, \boldsymbol{D}_1 + \boldsymbol{E}_{2,1}\}$,

iii) $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{E}_{1,2} + \boldsymbol{E}_{2,1}, \boldsymbol{D}_1 + \boldsymbol{E}_{1,2} + \boldsymbol{E}_{2,1}\}$.

Proof.

We have already established that for $supp(c) = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4\}$ there exists a permutation in $\mathfrak{H}(\ell,m)$ such that the image of $\{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4\}$ is $\{\mathbf{0}, \mathbf{D}_\rho, \mathbf{M}, \mathbf{D}_\rho + \mathbf{M}\}$, where $\rho = 1$ or $\rho = 2$ and $\mathbf{M}_{i,j} = 0$ for $i = j$ and for $i \geq 3$ or $j \geq 3$. If $\rho = 1$ then, $\mathbf{M} \in span_{\mathbf{F}_2}(\{\mathbf{E}_{1,2}, \mathbf{E}_{2,1}\})$. This implies the image of $supp(c)$ is in the required form. If $\rho = 2$ then, exactly one of $\mathbf{M}$ or $\mathbf{D}_\rho + \mathbf{M}$ is a zero of the 2-minor $f = det(\mathbf{X}_{\{1,2\},\{1,2\}})$. Since both $\mathbf{M}$ and $\mathbf{D}_\rho + \mathbf{M}$ only have nonzero entries at the positions $(1,1),(1,2),(2,1),(2,2)$ all other 2-minors vanish at the four matrices. Therefore, the matrix which is a zero of $f = det(\mathbf{X}_{\{1,2\},\{1,2\}})$ is a matrix of rank 1. We may find an automorphism in $\mathfrak{H}(\ell,m)$ to map the rank 1 matrix to $\mathbf{D}_1$. □

The three cases in the above theorem are representatives of all possible orbits of supports of weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ arising under the action of the group $\mathfrak{H}(\ell,m)$. This means we can describe any support of a minimum weight codeword rather explicitly. We state this in the following corollary:

Corollary 6.1.15 *The support of a minimum weight codeword of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ is among one of the following three distinct classes of supports:*

i) $\{\boldsymbol{U}, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_1, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_2, \boldsymbol{U} + \boldsymbol{b}_1^T(\boldsymbol{a}_1 + \boldsymbol{a}_2)\}$,

ii) $\{\boldsymbol{U}, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_1, \boldsymbol{U} + \boldsymbol{b}_2^T\boldsymbol{a}_1, \boldsymbol{U} + (\boldsymbol{b}_1 + \boldsymbol{b}_2)^T\boldsymbol{a}_1\}$,

iii) $\{\boldsymbol{U}, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_1, \boldsymbol{U} + \boldsymbol{b}_1^T\boldsymbol{a}_2 + \boldsymbol{b}_2^T\boldsymbol{a}_1, \boldsymbol{U} + (\boldsymbol{b}_1^T\boldsymbol{a}_1 + \boldsymbol{b}_2^T\boldsymbol{a}_1 + \boldsymbol{b}_1^T\boldsymbol{a}_2)\}$.

Here $\boldsymbol{U} \in \mathbb{M}^{\ell\times\ell'}(\mathbf{F}_2)$, while $\{\boldsymbol{a}_1, \boldsymbol{a}_2\} \subset \mathbf{F}_2^{\ell'}$ and $\{\boldsymbol{b}_1, \boldsymbol{b}_2\} \subset \mathbf{F}_2^{\ell}$ are two pairs of linearly independent vectors. Conversely, any such set occurs as the support set of a minimum weight codeword in $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$.

Proof.

Acting on the three representatives from Theorem 6.1.14 with $\sigma_{\mathbf{U},\mathbf{A},\mathbf{B}}$ gives a description of all possible support sets. The matrix $\mathbf{M} := \mathbf{B}\mathbf{D}_1\mathbf{A}$ is of the form $\mathbf{M} = \mathbf{b}_1^T\mathbf{a}_1$ for certain non-zero vectors $\mathbf{b}_1, \mathbf{a}_1$. In fact, $\mathbf{b}_1^T$ is the first column of $\mathbf{B}$ and $\mathbf{a}_1$ is first row of $\mathbf{A}$. Similarly, $\mathbf{B}\mathbf{E}_{1,2}\mathbf{A} = \mathbf{b}_1^T\mathbf{a}_2$ and $\mathbf{B}\mathbf{E}_{2,1}\mathbf{A} = \mathbf{b}_2^T\mathbf{a}_1$, with $\mathbf{b}_2^T$ (resp. $\mathbf{a}_2$) the second column of $\mathbf{B}$ (resp. the second row of $\mathbf{A}$). Note that $\mathbf{b}_1$ and $\mathbf{b}_2$ (resp. $\mathbf{a}_1$ and $\mathbf{a}_2$) necessarily are linearly independent, since $\mathbf{B}$ (resp. $\mathbf{A}$) is an invertible matrix. (This shows the first part of the corollary.) Since $\mathbf{A}$ and $\mathbf{B}$ may be chosen freely any set of the given three forms occurs as the support set of a minimum weight codeword. □

A geometric description of this corollary is that the support sets lie on a coset of certain subspaces of $\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_2)$ of dimension two. The subspaces are not arbitrary, but are generated by matrices of a specific form. This enables us to count the number of weight 4 codewords in $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$.

Corollary 6.1.16 *The number of minimum weight codewords of* $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ *is*

$$\frac{(2^{\ell}-1)(2^{\ell'}-1)2^{\delta-2}}{3}\left((2^{\ell-1}-1)+(2^{\ell'-1}-1)+3(2^{\ell-1}-1)(2^{\ell'-1}-1)\right).$$

Proof.

We first count the number of possible supports of type i). As the first step we determine the number of possibilities for the 2-dimensional subspace

$$W_1 := \{\mathbf{0}, \mathbf{b}_1^T\mathbf{a}_1, \mathbf{b}_1^T\mathbf{a}_2, \mathbf{b}_1^T(\mathbf{a}_1+\mathbf{a}_2)\}.$$

We may choose $\mathbf{b}_1$ in $2^{\ell}-1$ distinct ways. Rather than choosing the vectors $\mathbf{a}_1$ and $\mathbf{a}_2$, we simply choose a 2-dimensional subspace of $\mathbf{F}_2^{\ell'}$. This can be done in $(2^{\ell'}-1)(2^{\ell'}-2)/6$ ways. For W_1 there are the following number of possible choices:

$$\frac{(2^{\ell}-1)(2^{\ell'}-1)(2^{\ell'-1}-1)}{3}.$$

Since each W_1 has exactly $2^{\delta-2}$ distinct cosets, this gives a total of

$$\frac{2^{\delta-2}(2^{\ell}-1)(2^{\ell'}-1)(2^{\ell'-1}-1)}{3}$$

possibilities for the support in case i). Similarly in case ii) one obtains

$$\frac{2^{\delta-2}(2^{\ell'}-1)(2^{\ell}-1)(2^{\ell-1}-1)}{3}$$

possibilities.

The last case left to investigate is case iii). We first wish to determine the number of possibilities for

$$W_2 := \{\mathbf{0}, \mathbf{b}_1^T\mathbf{a}_1, \mathbf{b}_1^T\mathbf{a}_2+\mathbf{b}_2^T\mathbf{a}_1, \mathbf{b}_1^T\mathbf{a}_1+\mathbf{b}_1^T\mathbf{a}_2+\mathbf{b}_2^T\mathbf{a}_1\}.$$

Note that W_2 contains exactly one matrix of rank one, which is determined uniquely by choosing $\mathbf{b}_1$ and $\mathbf{a}_1$ since $q=2$. Therefore, the rank one matrix can

be chosen in $(2^{\ell}-1)(2^{\ell'}-1)$ distinct ways. The vector $\mathbf{b}_2$ (resp. $\mathbf{a}_2$) should be chosen linearly independent from $\mathbf{b}_1$ (resp. $\mathbf{a}_1$) and there are as such $2^{\ell'-2}$ (resp. $2^{\ell'}-2$) possibilities. However, different choices can give rise to the same subspace W_2. If

$$\mathbf{b}_1^T\mathbf{a}_2 + \mathbf{b}_2^T\mathbf{a}_1 = \mathbf{b}_1^T\mathbf{a}_2' + (\mathbf{b}_2')^T\mathbf{a}_1,$$

then

$$\mathbf{b}_1^T(\mathbf{a}_2 + \mathbf{a}_2') = (\mathbf{b}_2 + \mathbf{b}_2')^T\mathbf{a}_1,$$

implying that $\mathbf{a}_2+\mathbf{a}_2' = 0$ and $\mathbf{b}_2+\mathbf{b}_2' = 0$ or that $\mathbf{a}_2+\mathbf{a}_2' = \mathbf{a}_1$ and $\mathbf{b}_1 = \mathbf{b}_2+\mathbf{b}_2'$. Similarly, if

$$\mathbf{b}_1^T\mathbf{a}_1 + \mathbf{b}_1^T\mathbf{a}_2 + \mathbf{b}_2^T\mathbf{a}_1 = \mathbf{b}_1^T\mathbf{a}_2' + (\mathbf{b}_2')^T\mathbf{a}_1,$$

then either $\mathbf{a}_2' = \mathbf{a}_1 + \mathbf{a}_2 = 0$ and $\mathbf{b}_2' = \mathbf{b}_2 = 0$ or $\mathbf{a}_2' = \mathbf{a}_2$ and $\mathbf{b}_2' = \mathbf{b}_1 + \mathbf{b}_2$. This brings the total number of possibilities for the choice of W_2 to:

$$\frac{(2^{\ell}-1)(2^{\ell'}-1)(2^{\ell}-2)(2^{\ell'}-2)}{4}.$$

The rest of the counting is then done as before. Adding all contributions from the three cases together, one obtains the corollary. □

We can use the classification theorem to count the number of codewords of weight 4 in each orbit of the automorphism group. Although once we could generate $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ with its weight 4 codewords meant that we could consider $\mathcal{C}^{\mathbb{A}}(\ell, m)$ as a Tanner code using Definition 3.3.5. We went through the trouble of classifying and counting the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ for several reasons. Empirically, we have decoded $\mathcal{C}^{\mathbb{A}}(\ell, m)$ by using the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ and the iterative decoder coming from the Tanner graph. Therefore for decoding purposes, as well as for the geometry given by the codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ of weight 4, we are interested in counting the codewords which contain a 1 in a fixed position, as well as counting the codewords in which two fixed positions contain 1. For this purpose, we have the following theorem.

Theorem 6.1.17 *The number of minimum weight codewords in $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$ which contain a 1 in position $\boldsymbol{0}$ equals*

$$\frac{(2^{\ell}-1)(2^{\ell'}-1)}{3}\left((2^{\ell-1}-1) + (2^{\ell'-1}-1) + 3(2^{\ell-1}-1)(2^{\ell'-1}-1)\right).$$

To find the number of codewords with support in the pair $\mathbf{0}, \mathbf{D}_1$, we will use the following lemma.

Lemma 6.1.18 *Let $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{A}, \boldsymbol{D}_1+\boldsymbol{A}\}$ and $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{B}, \boldsymbol{D}_1+\boldsymbol{B}\}$ be two distinct sets of supports of codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^{\perp}$. Then $\{\boldsymbol{0}, \boldsymbol{D}_1, \boldsymbol{A}+\boldsymbol{B}, \boldsymbol{D}_1+\boldsymbol{A}+\boldsymbol{B}\}$*

is also the set of support of a codeword of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$. *Moreover, the number of minimum weight codewords in* $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ *which contain a* 1 *in positions* $\boldsymbol{0}, \boldsymbol{D}_1$ *equals* $2^{\ell+\ell'-2}-1$.

Using similar arguments we obtain the following theorem.

Theorem 6.1.19 *The number of minimum weight codewords in* $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ *which contain a* 1 *in positions* $\boldsymbol{0}, \boldsymbol{D}_2$ *equals* 2^2-1.

6.1.3 Affine Grassmann codes as Tanner codes

Since we have determined the minimum weight codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ we can use this information to study $\mathcal{C}^{\mathbb{A}}(\ell,m)$ as a Tanner code in a natural way. For the binary case we can use Definition 3.3.5 to make a bipartite graph with the minimum weight codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$. Clearly, $\mathcal{C}^{\mathbb{A}}(\ell,m)$ is the Tanner code coming from this graph and a $[4,3,2]$ component code. In the remainder of this section we focus on the nonbinary case, i.e. $q \neq 2$.

Definition 6.1.20 *A* line *of* $\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$ *is a set of the form* $Span_{\mathbf{F}_q}(\boldsymbol{M})+\boldsymbol{U}$, *where* $\boldsymbol{M}, \boldsymbol{U} \in \mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$ *and* $\boldsymbol{M}$ *has rank* 1. *We denote the set of lines by* $\mathcal{L}(\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q))$.

Note that there are $\frac{(q^{\ell}-1)(q^{\ell'}-1)}{(q-1)^2}q^{\ell\ell-1}$ lines. Each matrix of $\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$ is contained in $\frac{(q^{\ell}-1)(q^{\ell'}-1)}{(q-1)^2}$ lines. Each line contains q matrices. We can construct a graph relating the matrices and the lines as follows.

Definition 6.1.21 *We define* Γ_3 *as follows. The vertices in* $V_1(\Gamma_3)$ *are the matrices in* $\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q)$. *The vertices in* $V_2(\Gamma_3) := \mathcal{L}(\mathbb{M}^{\ell\times\ell'}(\mathbf{F}_q))$. *The edges* $E(\Gamma_3) := \{(\boldsymbol{A}, Span_{\mathbf{F}_q}(\boldsymbol{B})+\boldsymbol{C}) \mid \boldsymbol{A}-\boldsymbol{C} \in Span_{\mathbf{F}_q}(\boldsymbol{B})\}$. *We call* Γ_3 *the* point–line graph of the affine Grassmannian.

We use the following labelings to make Γ_3 a $(\frac{(q^{\ell}-1)(q^{\ell'}-1)}{(q-1)^2}, q)$-regular bipartite endpoint labeled graph.

For each line $Span_{\mathbf{F}_q}(\mathbf{B})+\mathbf{C}$ fix $\alpha \in \mathbf{F}_q^*$. The labeling $\phi_{Span_{\mathbf{F}_q}(\mathbf{B})+\mathbf{C}}$ assigns to $\mathbf{A} = \gamma\alpha\mathbf{B}+\mathbf{C}$ the $\mathbf{F}_q$ element γ. Now we have the following theorem.

Theorem 6.1.22 *For $q \neq 2$*

$$\mathcal{C}^{\mathbb{A}}(\ell,m) = (\Gamma_3, RS(\mathbf{F}_q,2)).$$

Proof.

Let c be a codeword of $\mathcal{C}^{\mathbb{A}}(\ell,m)$. Consider the values of the codeword c at the line $Span_{\mathbf{F}_q}(\mathbf{B}) + \mathbf{C} \in \mathcal{L}(\Gamma_3)$. Let $\alpha_1 \in \mathbf{F}_q^*$ be the nonzero element chosen for $\phi_{Span_{\mathbf{F}_q}(\mathbf{B})+\mathbf{C}}$. We may apply an automorphism of $\mathfrak{H}(\ell,m)$ to consider the values of a codewords c' on the line $Span_{\mathbf{F}_q}(\mathbf{E}_{1,1})$. Let α_2 be the nonzero element chosen for $\phi_{Span_{\mathbf{F}_q}(\mathbf{E}_{1,1})}$. Since there is an automorphism which maps $\gamma\alpha_1\mathbf{B} + \mathbf{C}$ to $\gamma\alpha_2\mathbf{E}_{1,1}$, the labeling $\phi_{Span_{\mathbf{F}_q}(\mathbf{B})+\mathbf{C}}(\gamma\alpha_1\mathbf{B} + \mathbf{C}) = \gamma$ is equal to $\phi_{Span_{\mathbf{F}_q}(\mathbf{E}_{1,1})}(\gamma\alpha_2\mathbf{E}_{1,1}) = \gamma$. The codeword c' evaluates to a codeword in $RS(\mathbf{F}_q,2)$ over the line $Span_{\mathbf{F}_q}(\mathbf{E}_{1,1})$ we have that $\mathcal{C}^{\mathbb{A}}(\ell,m) \subseteq (\Gamma_3, RS(\mathbf{F}_q,2))$.

For the reverse implication we prove $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp} \subseteq (\Gamma_3, RS(\mathbf{F}_q,2))^{\perp}$ as follows: A weight 3 codeword of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ has support completely contained inside a line $Span_{\mathbf{F}_q}(\mathbf{B}) + \mathbf{C} \in \mathcal{L}(\Gamma_3)$. Therefore, it is also a parity check of $(\Gamma_3, RS(\mathbf{F}_q,2))^{\perp}$. The subcode of weight 3 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ is contained in $(\Gamma_3, RS(\mathbf{F}_q,2))^{\perp}$. Since the code generated but the weight 3 codewords is the full code $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$, we have that $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp} \subseteq (\Gamma_3, RS(\mathbf{F}_q,2))^{\perp}$. □

Unfortunately, we have not been able to use this description to decode $\mathcal{C}^{\mathbb{A}}(\ell,m)$ completely.

6.2 Codewords of $\mathcal{C}(\ell,m)^{\perp}$

Definition 6.2.1 *Let $V := \mathbf{F}_q^m$. We define $\mathcal{G}_{\ell,m}$ as the set of all ℓ dimensional subspaces of V.*

Definition 6.2.2 *We denote $\#\mathcal{G}_{\ell,m}$ by $\begin{bmatrix} m \\ \ell \end{bmatrix}_q$.*

A counting argument shows

$$\begin{bmatrix} m \\ \ell \end{bmatrix}_q = \prod_{i=0}^{\ell-1} \frac{q^{m-i}-1}{q^{\ell-i}-1}.$$

Closely related to the affine Grassmann codes are the Grassmann codes which we define now.

Definition 6.2.3 *Let m be an integer. Suppose $\ell \leq m$. For each $W \in \mathcal{G}_{\ell,m}$ pick an $\ell \times m$ matrix whose rowspace is W. Denote this matrix by $\boldsymbol{M}_W$. Denote the set of all such chosen matrices as $\mathbb{M}(\mathcal{G}_{\ell,m})$. Let $\boldsymbol{Y}$ be an $\ell \times m$ matrix on the ℓm indeterminates $Y_{i,j}$. We define the Grassmann code $\mathcal{C}(\ell, m)$ as the affine variety code $C(\mathbb{M}(\mathcal{G}_{\ell,m}), Span_{\mathbf{F}_q}(\det \ell(\boldsymbol{Y}_J)))$.*

The Grassmann codes were introduced in [Rya87a] and [Rya87b] for the binary case and for general q in [Nog93]. Grassmann codes are a $[\begin{bmatrix} m \\ \ell \end{bmatrix}_q, \binom{m}{\ell}, q^{\ell(m-\ell)}]_q$ code. Note that a specific $\mathcal{C}(\ell, m)$ code depends on the exact matrices in $\mathbb{M}(\mathcal{G}_{\ell,m})$. Therefore we may pick a single Grassmann code from a monomially equivalent class. We also refer to the class of monomially equivalent codes as Grassmann codes.

We may consider $\mathcal{C}^{\mathbb{A}}(\ell, m)$ as a projection of $\mathcal{C}(\ell, m)$. For $\mathbf{M} \in \mathbb{M}^{\ell \times \ell'}(\mathbf{F}_q)$ let $\mathbf{M'} = (\mathbf{I}_\ell | \mathbf{M}) \in \mathbb{M}^{\ell \times m}(\mathbf{F}_q)$. The h-minors, for $0 \leq h \leq \ell$ of the indeterminate $\ell \times \ell'$ matrix $\mathbf{X}$ are also ℓ-minors of the $\ell \times m$ matrix $\mathbf{X'} = (\mathbf{I}_\ell | \mathbf{X})$. We denote the affine Grassmannian $\mathcal{G}^{\mathbb{A}}_{\ell,m} := \{W \in \mathcal{G}_{\ell,m} |\ \mathbf{M}_W = (\mathbf{I}_\ell | \mathbf{M}) \in \mathbb{M}^{\ell \times m}(\mathbf{F}_q)\}$. Therefore $\mathcal{C}^{\mathbb{A}}(\ell, m)$ is obtained from $\mathcal{C}(\ell, m)$ by evaluating the ℓ-minors of the matrices for the ℓ spaces in $\mathcal{G}^{\mathbb{A}}_{\ell,m}$.

From the properties of minors we know that $d(\mathcal{C}(\ell, m)^\perp) > 2$. In this section we show $d(\mathcal{C}(\ell, m)^\perp) = 3$ and we classify the minimum weight codewords of $\mathcal{C}(\ell, m)^\perp$. We begin with some definitions.

Definition 6.2.4 *[Pan10]*

Let $Z \in \mathcal{G}_{\ell-1,m}$ and $Z \in \mathcal{G}_{\ell+1,m}$, where $\ell + 1 \leq m$. A line of the Grassmannian *is defined as:*

$$\pi_Z^{Z'} := \{W \in \mathcal{G}_{\ell,m} \mid Z \subseteq W \subseteq Z'\}.$$

We denote the set of all such lines of the Grassmannian by $\mathcal{L}(\mathcal{G}_{\ell,m})$.

Note that there are a total of $\begin{bmatrix} m \\ \ell \end{bmatrix}_q \frac{(q^\ell - 1)(q^{m-\ell} - 1)}{(q-1)^2}$ lines. Also, any line of the Grassmannian is isomorphic to the line $\mathcal{G}_{1,2}$.

Definition 6.2.5 *The graph Γ_4 is the following $(\begin{bmatrix} m-\ell \\ 1 \end{bmatrix}_q \begin{bmatrix} \ell \\ 1 \end{bmatrix}_q, q+1)$-regular bipartite graph: $V_1(\Gamma_4) = \mathcal{G}_{\ell,m}$, $V_2(\Gamma_4) = \mathcal{L}(\mathcal{G}_{\ell,m})$ and the set of edges is $E(\Gamma_4) := \{(W, \pi_Z^{Z'}) \ | W \in \pi_Z^{Z'}\}$. This graph is also known as* the point–line graph of the Grassmannian.

THEOREM 6.2.6 *The group $\mathbf{GL}_m(\mathbf{F}_q)$ induces an automorphism of $\mathcal{C}(\ell,m)$ by mapping $W \in \mathcal{G}_{\ell,m}$ to $\boldsymbol{G}(W) \in \mathcal{G}_{\ell,m}$ for $\boldsymbol{G} \in \mathbf{GL}_m(\mathbf{F}_q)$. We will also consider the induced map given by $\boldsymbol{M}_V \mapsto \boldsymbol{M}_V \boldsymbol{G}$.*

Now we can classify the support of a nonzero codeword of $\mathcal{C}(\ell,m)^{\perp}$.

THEOREM 6.2.7 *Let V, W and U in $\mathcal{G}_{\ell,m}$. Then V, W and U are the nonzero positions of a codeword of a $\mathcal{C}(\ell,m)^{\perp}$ if and only if V, W and U belong to the same line.*

PROOF.

First we prove the converse. Suppose V, W and U are in the line $\pi_Z^{Z'}$. Then $Z = V \cap W \cap U$ and $Z' = span_{\mathbf{F}_q}(V + W + U)$. Then, there exist $\mathbf{x}$ and $\mathbf{y}$ such that $V = Span_{\mathbf{F}_q}(Z, \mathbf{x})$, $W = Span_{\mathbf{F}_q}(Z, \mathbf{y})$, $U = Span_{\mathbf{F}_q}(Z, \mathbf{x}+\mathbf{y})$ and the span of the three spaces is $Span_{\mathbf{F}_q}(V+W+U) = Span_{\mathbf{F}_q}(\{Z, \mathbf{x}, \mathbf{y}\})$. Since the determinant is a multilinear function we may find matrix representatives: $\mathbf{M}_V, \mathbf{M}_W$ and $\mathbf{M}_U$ such that $f(\mathbf{M}_V) + f(\mathbf{M}_W) - f(\mathbf{M}_U) = 0$ for any ℓ-minor $f = det(\mathbf{Y}_I)$. Since we have proven there is one Grassmann code, $\mathcal{C}(\ell,m)^{\perp}$, which has V, W and U as support of a weight 3 codeword, we have also proven it for any other monomially equivalent Grassmann code.

Now we prove the direct implication. Let V, W and U be three vector spaces in $\mathcal{G}_{\ell,m}$ such that, V, W and U represent the nonzero positions of a codeword of a $\mathcal{C}(\ell,m)^{\perp}$. We represent the vector spaces by the matrices $\mathbf{M}_V, \mathbf{M}_W$ and $\mathbf{M}_U$. The nonzero coefficients of $\mathbf{c}$ are: c_V, c_W and c_U.

We pick $\mathbf{G} \in \mathbf{GL}_m(\mathbf{F}_q)$ such that $\mathbf{M}_V\mathbf{G} = (\mathbf{I}_\ell|\mathbf{0})$. Let $J := \{1, 2, \ldots, \ell\}$ and consider the ℓ-minor $f = det(\mathbf{Y}_J)$. Since $f(\mathbf{M}_V) = 1$ and c_V, c_W, c_U are nonzero then we may assume $f(\mathbf{M}_W) \neq 0$. We apply row operations to $\mathbf{M}_W$ such that $f(\mathbf{M}_W) = 1$. The row operations correspond to choosing different representative matrices of the elements in $\mathcal{G}_{\ell,m}$. After these row operations we have changed the particular Grassmann code, but this is irrelevant since we have not fixed the nonzero entries of $\mathbf{c}$.

Now we assume $c_V = c_U = 1$, $c_W = -1$. In addition we may assume $f(\mathbf{M}_U) \neq 1$. Since $f_J(\mathbf{M}_W) = 1$ we apply $G = \left(\begin{smallmatrix} \mathbf{I}_\ell & \mathbf{0} \\ \mathbf{C} & \mathbf{B} \end{smallmatrix}\right) \in \mathbf{GL}_m(\mathbf{F}_q)$ simultaneously to all matrices on the last $m - \ell$ columns of $\mathbf{M}_V$ are unchanged but,

$$\mathbf{M}_W = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & n_{1,\ell+1} & \cdots & n_{1,m} \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 & n_{2,\ell+1} & \cdots & n_{2,m} \\ \vdots & 0 & \ddots & 0 & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & 0 & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & n_{\ell,\ell+1} & \cdots & n_{\ell,m} \end{array}\right).$$

Let $J' = J \cup \{\ell+1\} \setminus \{i\}$. If $f = det(\mathbf{Y}_{J'})$ is the ℓ-minor on the columns of J', then $f(\mathbf{M}_V) + f(\mathbf{M}_W) - f(\mathbf{M}_U) = 0$. Thus $f(\mathbf{M}_W) = f(\mathbf{M}_U) = 1$. Therefore, we may apply row operations to $\mathbf{M}_U$ such that,

$$\mathbf{M}_U = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & o_{1,i} & 0 & \cdots & 0 & 0 & \cdots & o_{1,m} \\ 0 & 1 & \cdots & o_{2,i} & 0 & \cdots & 0 & 0 & \cdots & o_{2,m} \\ \vdots & 0 & \ddots & & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{i,i} & 0 & \cdots & 0 & 1 & \cdots & o_{i,m} \\ \vdots & 0 & \cdots & o_{i+1,1} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & o_{\ell,m} \end{array}\right).$$

Note that $f(\mathbf{M}_U) = o_{i,i} \neq 1$. We will use the other ℓ-minors to determine the entries of $\mathbf{M}_W$ and $\mathbf{M}_U$. From now on, we let $1 \leq j \leq \ell$, and $j \neq i$ and $\ell + 1 < j' \leq m$.

For $J^* = J \cup \{j'\} \setminus \{i\}$ and for an ordering of the elements of J^* let $f = det(\mathbf{Y}_{J^*})$ be the ℓ-minor on the columns of J^*. If $f(\mathbf{M}_W) = 0$ and $f(\mathbf{M}_U) = o_{i,j'}$ then,

$$\mathbf{M}_U = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & o_{1,i} & 0 & \cdots & 0 & 0 & \cdots & o_{1,m} \\ 0 & 1 & \cdots & o_{2,i} & 0 & \cdots & 0 & 0 & \cdots & o_{2,m} \\ \vdots & 0 & \ddots & & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{i,i} & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & o_{i+1,1} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{\ell,i} & 0 & \cdots & 1 & 0 & \cdots & o_{\ell,m} \end{array}\right).$$

For $J^* = J \cup \{\ell+1\} \setminus \{j\}$ and $f = det(\mathbf{Y}_{J^*})$ we have that

$f(\mathbf{M}_W) = \begin{vmatrix} n_{j,i} & n_{j,\ell+1} \\ n_{i,i} & n_{i,\ell+1} \end{vmatrix}$ and $f(\mathbf{M}_U) = \begin{vmatrix} o_{j,i} & o_{j,\ell+1} \\ o_{i,i} & o_{i,\ell+1} \end{vmatrix}$. Since we have determined that $n_{j,i} = o_{j,\ell+1} = 0$ and $n_{i,i} = o_{i,\ell+1} = 1$, we have $f(\mathbf{M}_W) = -n_{j,\ell+1}$

and $f(\mathbf{M}_U) = o_{j,i}$. This implies

$$\mathbf{M}_U = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & -n_{1,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & o_{1,m} \\ 0 & 1 & \cdots & -n_{2,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & o_{2,m} \\ \vdots & 0 & \ddots & & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{i,i} & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & -n_{i+1,\ell+1} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -n_{\ell,\ell+1} & 0 & \cdots & 1 & 0 & \cdots & o_{\ell,m} \end{array}\right).$$

For $J^* = J \cup \{\ell+1, j'\} \setminus \{i, j\}$ and $f = det(\mathbf{Y}_{J^*})$ we have that $f(\mathbf{M}_W) = n_{j,j'}$ and $f(\mathbf{M}_U) = o_{j,j'}$. Therefore

$$\mathbf{M}_U = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & -n_{1,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & n_{1,m} \\ 0 & 1 & \cdots & -n_{2,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & n_{2,m} \\ \vdots & 0 & \ddots & & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{i,i} & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & -n_{i+1,\ell+1} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -n_{\ell,\ell+1} & 0 & \cdots & 1 & 0 & \cdots & n_{\ell,m} \end{array}\right).$$

For $J^* = J \cup \{j'\} \setminus \{j\}$ and $f = det(\mathbf{Y}_{J^*})$ we have that $f(\mathbf{M}_W) = n_{j,j'}$ and $f(\mathbf{M}_U) = o_{i,i} n_{j,j'}$. Since $f(\mathbf{M}_W) = f(\mathbf{M}_U)$ and $o_{i,i} \neq 1$ we have $f(\mathbf{M}_W) = 0$. Therefore,

$$\mathbf{M}_W = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & n_{1,\ell+1} & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 & n_{2,\ell+1} & \cdots & 0 \\ \vdots & 0 & \ddots & 0 & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & 0 & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & n_{\ell,\ell+1} & \cdots & 0 \end{array}\right).$$

$$\mathbf{M}_U = \left(\begin{array}{ccccccc|ccc} 1 & 0 & \cdots & -n_{1,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & -n_{2,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & o_{i,i} & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & -n_{i+1,\ell+1} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -n_{\ell,\ell+1} & 0 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right).$$

Now we perform row operations on $\mathbf{M}_W$ to put it in the following form

$$\mathbf{M}_W = \left(\begin{array}{cccccccc|ccc} 1 & 0 & \cdots & -n_{1,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & -n_{2,\ell+1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & & 0 & \cdots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & 0 & \cdots & -n_{i+1,\ell+1} & 1 & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & -n_{\ell,\ell+1} & 0 & \cdots & 1 & 0 & \cdots & 0 \end{array}\right).$$

Now that we have determined $\mathbf{M}_V$, $\mathbf{M}_W$ and $\mathbf{M}_W$ completely we can clearly identify their rowspaces V, W and U. Note that all entries except those in row i are the same for the three matrices. Therefore, $dim(V \cap W \cap U) = \ell - 1$. Since the i-th row of $\mathbf{U}$ is a linear combination of the i-th row of $\mathbf{M}_V$ and $\mathbf{W}$ the fact $dim\ span_{\mathbf{F}_q}(V + W + U) = \ell + 1$ follows. Which implies V, W and U belong to the line given by $V \cap W \cap U$ and $span_{\mathbf{F}_q}(V + W + U)$. □

As a corollary we can easily count the minimum weight codewords of $\mathcal{C}(\ell, m)^\perp$.

Corollary 6.2.8 *The code $\mathcal{C}(\ell, m)^\perp$ has*

$$\frac{(q^\ell - 1)(q^{m-\ell} - 1)q}{3!} \begin{bmatrix} m \\ \ell \end{bmatrix}_q$$

codewords of weight 3.

Proof.

There are $\frac{q^{m-\ell}-1}{q-1}\begin{bmatrix} m \\ \ell \end{bmatrix}_q \begin{bmatrix} \ell+1 \\ \ell-1 \end{bmatrix}_q$ lines in $\mathcal{L}(\mathcal{G}_{\ell,m})$. Each line contains $q+1$ elements of $\mathcal{G}_{\ell,m}$. Each of the $\binom{q+1}{3}$ subsets of the lines is the support of a weight 3 codeword. For each set of 3 elements there are $q-1$ codewords of weight 3. □

This is quite similar to the formula of weight 3 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$. We end this section with a proof that the Grassmann codes are Tanner codes of Γ_4. Recall that for a linear space $W \subset \mathbf{F}_q^A$ and $B \subseteq A$ we represent the projection of W onto B by W^B. Note that the elements of the Grassmannian are all codes of dimension ℓ contained in $\mathbf{F}_q^{\{1,2,\ldots,m\}}$. For the purposes of this section, we shall consider $B = \{1, 2, \ldots, \ell\}$.

Definition 6.2.9 *We define*

$$\mathcal{G}_{\ell,m}^{\ell-h} := \{W \in \mathcal{G}_{\ell,m} \mid \dim W^B = h\}.$$

Note that we may partition $\mathcal{G}_{\ell,m}$ with the sets $\mathcal{G}_{\ell,m}^{h}$ for $h = 0, 1, \ldots, \ell$. Also note that $\mathcal{G}_{\ell,m}^{\mathbb{A}} = \mathcal{G}_{\ell,m}^{0}$.

Lemma 6.2.10 *Let $W \in \mathcal{G}_{\ell,m}^{h}$ where $h > 0$. There exist $U, V \in \mathcal{G}_{\ell,m}^{h-1}$ such that U, V and W lie on the same line.*

Proof.

Let $W \in \mathcal{G}_{\ell,m}^{h}$ where $0 < h$. There exists $x \in W$ such that the projection of x onto B is 0. Since $\dim W^B < \ell$ there exists $y \in \mathbf{F}_q$ such that the projection of y onto B is not in W^B. We may assume W is of the form $Span_{\mathbf{F}_q}(T \cup \{x\})$. Then $U = Span_{\mathbf{F}_q}(T \cup \{x+y\})$ and $V = Span_{\mathbf{F}_q}(T \cup \{y\})$ belong to $\mathcal{G}_{\ell,m}^{h-1}$. □

Now we consider the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ over $\mathbf{F}_2$ as codewords of $\mathcal{C}(\ell,m)^{\perp}$.

Lemma 6.2.11 *Let c be a codeword of weight 4 of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ over the binary field. Then the support of c is equal to the symmetric difference of two lines of $\mathcal{G}_{\ell,m}$ with a point in common.*

Proof.

From Theorem 6.1.14 we know that the support of the weight 4 codewords of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ over $\mathbf{F}_2$ follow in one of these three cases:

i) $\{\mathbf{0}, \mathbf{D}_1, \mathbf{E}_{1,2}, \mathbf{D}_1 + \mathbf{E}_{1,2}\}$,

ii) $\{\mathbf{0}, \mathbf{D}_1, \mathbf{E}_{2,1}, \mathbf{D}_1 + \mathbf{E}_{2,1}\}$,

iii) $\{\mathbf{0}, \mathbf{D}_1, \mathbf{E}_{1,2} + \mathbf{E}_{2,1}, \mathbf{D}_1 + \mathbf{E}_{1,2} + \mathbf{E}_{2,1}\}$.

Note that the automorphism induced by $\mathbf{X} \mapsto \mathbf{X} + \mathbf{U}$ of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ is induced by the induced automorphism $(\mathbf{X}|\mathbf{I}_\ell) \mapsto (\mathbf{X}|\mathbf{I}_\ell)\begin{pmatrix} \mathbf{I}_{m-\ell} & \mathbf{0} \\ \mathbf{U} & \mathbf{I}_\ell \end{pmatrix}$ of $\mathcal{C}(\ell,m)$. Additionally, note that the automorphism $\mathbf{X} \mapsto \mathbf{X}\mathbf{A}$ of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ is induced by the automorphism $(\mathbf{X}|\mathbf{I}_\ell) \mapsto (\mathbf{X}|\mathbf{I}_\ell)\begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_\ell \end{pmatrix}$ and the automorphism $\mathbf{X} \mapsto \mathbf{B}\mathbf{X}$ of $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$ is

induced by the automorphism $(\mathbf{X}|\mathbf{I}_\ell) \mapsto (\mathbf{X}|\mathbf{I}_\ell)\begin{pmatrix} \mathbf{I}_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{-1} \end{pmatrix}$. Therefore, the weight 4 codewords have the following positions in $\mathcal{G}_{\ell,m}$:

i) $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell), (\mathbf{E}_{1,2}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{1,2}|\mathbf{I}_\ell)\}$,

ii) $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell), (\mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$,

iii) $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell), (\mathbf{E}_{1,2} + \mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{1,2} + \mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$.

Note that each pair of linear spaces $\{(\mathbf{0}|\mathbf{I}_\ell), (\mathbf{D}_1|\mathbf{I}_\ell)\}$, $\{(\mathbf{E}_{1,2}|\mathbf{I}_\ell), (\mathbf{D}_1+\mathbf{E}_{1,2}|\mathbf{I}_\ell)\}$, $\{(\mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$ and $\{(\mathbf{E}_{1,2} + \mathbf{E}_{2,1}|\mathbf{I}_\ell), (\mathbf{D}_1 + \mathbf{E}_{1,2} + \mathbf{E}_{2,1}|\mathbf{I}_\ell)\}$ are contained in a line of $\mathcal{L}(\mathcal{G}_{\ell,m})$ and the third point of each line is $(\mathbf{D}_1|\mathbf{I}_\ell - \mathbf{D}_1)$. □

Theorem 6.2.12 *Let c be a codeword of weight 4 of $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$ over a non-binary field. Then the support of c is equal to the 3 points on a line of $\mathcal{G}_{\ell,m}$.*

Proof.

From Theorem 6.1.14, we know that the support of the weight 3 codewords of $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$ over $\mathbf{F}_q$ have support in the orbit of $\{\mathbf{0}, \mathbf{M}, \alpha\mathbf{M}\}$ where $\mathbf{M}$ has rank 1. As we saw in the proof of Lemma 6.2.11, we may consider the group of induced automorphisms $\mathfrak{H}(\ell, m)$ as the group of automorphisms of $\mathcal{G}_{\ell,m}$ generated by $\begin{pmatrix} \mathbf{I}_{m-\ell} & \mathbf{0} \\ \mathbf{U} & \mathbf{I}_\ell \end{pmatrix}$, $\begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_\ell \end{pmatrix}$ and $\begin{pmatrix} \mathbf{I}_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^{-1} \end{pmatrix}$. We may apply an automorphism from $\mathfrak{H}(\ell, m)$ to obtain the set $\{\mathbf{0}, \mathbf{E}_{1,1}, \alpha\mathbf{E}_{1,1}\}$. We consider the corresponding positions in $\mathcal{G}_{\ell,m}$ given by the matrices $\{(\mathbf{I}_\ell|\mathbf{0}), (\mathbf{I}_\ell|\mathbf{E}_{1,1}), (\mathbf{I}_\ell|\alpha\mathbf{E}_{1,1})\}$. Clearly, these three points lie on the same line. □

Theorem 6.2.13 *The code $\mathcal{C}(\ell, m)^\perp$ is generated by its minimum weight codewords.*

Proof.

Let $W \in \mathcal{G}_{\ell,m}$. The code $\mathcal{C}^{\mathbb{A}}(\ell, m)^\perp$ is generated by weight 3 codewords of $\mathcal{C}(\ell, m)^\perp$. Let $h > 0$. For each $W \in \mathcal{G}^h_{\ell,m}$, we can find a codeword of weight 3 of $\mathcal{C}(\ell, m)^\perp$ whose other two positions in its support lie in $\mathcal{G}^{h-1}_{\ell,m}$. This implies that

we have $\#\mathcal{G}_{\ell,m} - \#\mathcal{G}^0_{\ell,m}$ independent codewords, in addition from those from $\mathcal{C}^{\mathbb{A}}(\ell,m)^{\perp}$. Therefore, $\mathcal{C}(\ell,m)^{\perp}$ is generated by its weight 3 codewords. □

In order to express $\mathcal{C}(\ell,m)$ as a Tanner code, we need to consider the fact that $\mathcal{C}(\ell,m)$ is not a single code, but a class of monomially equivalent codes. For this pupose, we relax the definition of a Tanner code. A Tanner code should not be considered as having a single fixed code as a component code for the check nodes, but for each check node we pick, in addition to the labeling, a monomially equivalent code to the component code $\mathcal{C}(1,2)$. Most of the theory of graph codes is consistent with this definition as well.

Corollary 6.2.14

$$\mathcal{C}(\ell,m) = (\Gamma_4, \mathcal{C}(1,2)).$$

Proof.

Let c be a codeword of $\mathcal{C}(\ell,m)$. Consider the values of the codeword c at any line $\pi_Z^{Z'} \in \mathcal{L}(\mathcal{G}_{\ell,m})$. Since $\pi_Z^{Z'} = \mathcal{G}_{1,2}$, the codeword c at $\pi_Z^{Z'}$ is $\mathcal{C}(1,2)$. Therefore, there exists a vertexwise labelinng of Γ_4 and some choices of monomially equivalent codes to $\mathcal{C}(1,2)$ such that $\mathcal{C}(\ell,m) \subseteq (\Gamma_4, \mathcal{C}(1,2))$. Since $\mathcal{C}(\ell,m)^{\perp}$ is generated by its weight 3 codewords, and those weight 3 codewords have support in a line of the Grassmannian, and any weight 3 codewords on a line are also a parity check for a $\mathcal{G}_{1,2}$ code on that line we have $\mathcal{C}(\ell,m)^{\perp}$ is contained in $(\Gamma_4, \mathcal{C}(1,2))^{\perp}$ which finishes the proof. □

6.2.1 Iterative encoding of Grassmann codes

In this section we adapt the (k_1,k_2) forcing set of a bipartite graph G to work with Tanner codes instead of graph codes. Although everything can be stated in terms of graph based codes and forcing sets on the edges of Γ_4, we will give a definition of everyting specifically for Tanner codes.

Now we introduce the concept of a forcing set. Essentially a forcing set is a set of positions of the Tanner code (G,C) with the property that any codeword of any Tanner code with any labeling and any MDS component code is determined by the values at the positions corresponding to the forcing set or such a codeword does not exist.

Definition 6.2.15 *Let G be an (n_1, n_2)-regular graph. Let k be an integer satisfying $k \leq n_2$. Let $T \subseteq V_1(G)$. We say T is* k-closed *if T satisfies:*

$$\forall u \in V_2(G) \ \#(T \cap \mathcal{N}(u)) \geq k \rightarrow \mathcal{N}(u) \subseteq T.$$

That is, if there are at least k vertices adjacent to $u \in V_2(G)$ contained in T then, all n_2 vertices adjacent to u are also contained in T.

Theorem 6.2.16 *Let G be an (n_1, n_2)-regular graph and pick $k \leq n_2$. Let $S \subseteq V_1(G)$. There exists an unique smallest k-closed set containing S.*

Proof.

We define Z as follows:

- $Z = S \cup \mathcal{N}(u_1) \cup \mathcal{N}(u_2) \cup \ldots, \mathcal{N}(u_a)$,
- $Z_0 := S$,
- $Z_i := S \cup \mathcal{N}(u_1) \cup \mathcal{N}(u_2) \cup \ldots \cup \mathcal{N}(u_i) \subseteq Z$ satisfies $Z_i \cap \mathcal{N}(u_{i+1}) \geq k$,
- Z is k-closed.

We claim that if Z' is another k-closed containing S then it must also contain Z. Suppose Z' is k-closed and Z contains S. Suppose $Z \nsubseteq Z'$ then there exists Z_i such that, $Z_i \subseteq Z'$ but $Z_{i+1} \nsubseteq Z'$. Since $Z_i \cap \mathcal{N}(z_{i+1}) \geq k$, it follows that $Z_{i+1} \subseteq Z'$. Therefore, $Z \subseteq Z'$. □

Definition 6.2.17 *Let G be an (n_1, n_2)-regular graph. Let k be an integer satisfying $k \leq n_2$. Let $S \subseteq V_1(G)$. We define the unique smallest k-closed set containing S as the* k-closure *of S. We denote it by $cl_k(S)$. If $cl_k(S) = V_1(G)$ we say S is an k* forcing set.

The following theorem relates the size of a k forcing set of G with the dimension of a Tanner code with an $[n_2, k_2, d_2]$ MDS component code.

Theorem 6.2.18 *Suppose G is an (n_1, n_2) regular bipartite graph. Let C_2 be an MDS code of length n_2 and dimension k_2. Let S be a k forcing set of G Then (G, C) is linearly isomorphic to $(G, C)^S$ and $\dim(G, C) \leq \#S$.*

PROOF.

Consider $(G, C)^S$, the projection of (G, C) onto S. There is a linear map from (G, C) to $(G, C)^S$ where we map $c = (c_i)_{i \in V_1(G)}$ to $c_S = (c_i)_{i \in S}$. We will prove the kernel is zero dimensional. Let c be a codeword of $(G, C))$ which is mapped to the zero codeword of $(G, C)^S$. Therefore, $c_i = 0$ for $i \in S$. For each $u \in V_2(G)$, once we know $c_i = 0$ for k vertices of $\mathcal{N}(u)$, we know $c_i = 0$ for all vertices of $\mathcal{N}(u)$. Therefore, the set of zero positions of the codeword c is $cl_k(S)$. Since S is a k forcing set of G all positions of c have the entry zero.

Since the linear map (G, C) to $(G, C)^S$ has a trivial kernel, the dimension of (G, C) is equal to the dimension of $(G, C)^S$ which is at most $\#S$. □

We also get a corollary to Theorem 6.2.18. This corollary is that we may encode (G, C) iteratively from a codeword in $(G, C)^S$ where S is a k forcing set of G and C is an MDS code of dimension k.

Please note that we have mentioned nothing about encoding $(G, C)^S$. Encoding $(G, C)^S$ will probably also be difficult. What we have proven is that once the positions of the codeword in $(G, C)^S$ have been determined, it might be possible to determine the positions of some other neighborghood which has at least k but not n_2 positions determined or might not be possible to extend the entries of the code in this way. We will prove that once we have encoded $(G, C)^S$ then those values can always be extended uniquely to (G, C).

THEOREM 6.2.19 *Suppose G is an (n_1, n_2) regular bipartite endpoint labeled graph. Let C be an MDS code of length n_2 and dimension k. Let S be a k forcing set of G. Then, a codeword $c' \in (G, C)^S$ may be extended uniquely to a codeword in (G, C).*

PROOF.

The set S is a k forcing set. There exist $S_0, S_1, \ldots, S_m \subseteq V_1(G)$ satisfying: $S_0 = S$, $S_m = V_1(G)$ and $S_i = S_{i-1} \cup \mathcal{N}(u_i)$, where $k \leq \#(S_{i-1} \cap \mathcal{N}(u_i)) < n_2$ and $u_i \in V_2(G)$.

Let ϕ_{S_i} denote the linear map from (G, C) to $(G, C)^{S_i}$. Since S_i is a k forcing set of G, then ϕ_{S_i} is a linear isomorphism.

Let $\phi_S(c) = c' \in (G, C)^S = (G, C)^{S_0}$. Now we suppose that we have extended c' to $\phi_{S_i}(c) \in (G, C)^{S_i}$ and we want to prove that we can extend it uniquely to a codeword of $(G, C)^{S_{i+1}}$. The only possibility is to extend $\phi_{S_i}(c)$ to $\phi_{S_{i+1}}(c)$

because the positions in $S_{i+1} \setminus S_i$ are determined by the entries in $\phi_{S_i}(c)$ and those positions are exactly the entries of $\phi_{S_{i+1}}(c)$. □

Definition 6.2.20 *Let $e_1, e_2, \ldots, e_m$ be a basis of $\mathbf{F}_q^m$. We define $S \subseteq \mathcal{G}_{\ell,m}$ to be the set of the $\binom{m}{\ell}$ spaces in $\mathcal{G}_{\ell,m}$ generated by the $\binom{m}{\ell}$ subsets of this set of basis elements.*

From the properties of the Plücker embedding, the ℓ spaces of S are information set of the Grassmann code $\mathcal{C}(\ell, m)$. We will finish this chapter by proving that in fact, S is a 2 forcing set of Γ_4 and that one may encode iteratively starting from S.

Theorem 6.2.21 *The set S is a 2-forcing set for Γ_4.*

Proof.

We prove it by induction on ℓ and m. For $\ell = 0$, $S = \mathcal{G}_{0,m} = \{\{0\}\}$ the theorem is vacuously true. For $m = \ell$, $S = \mathcal{G}_{\ell,\ell} = \{\mathbf{F}_q^\ell\}$ the theorem is also vacuously true.

Otherwise, we may suppose $0 < \ell$ and $\ell < m$. Let S be the $\binom{m}{\ell}$ spaces in $\mathcal{G}_{\ell,m}$ generated by the standard basis vectors. Let S_m be the subset of S consisting of the spaces containing e_m. Let S_{m-1} be the subset of S, whose ℓ spaces do not contain e_m.

By the induction hypothesis on m, the 2-closure of the vertex set S_{m-1} is the set of vertices $Z_{m-1} = \{W \in \mathcal{G}_{\ell,m} \mid W \subseteq Span(\{e_1, e_2, \ldots, e_{m-1}\})\}$. Moreover, by the induction hypothesis on ℓ, the 2-closure of S_m is the set of ℓ spaces $Z_m = \{W \in \mathcal{G}_{\ell,m} \mid e_m \in W\}$. Therefore, the 2-closure of S contains both Z_{m-1} and Z_m. Let $W \in \mathcal{G}_{\ell,m}$, but not in Z_{m-1} nor Z_m. Therefore $W = Span(Z \cup y + e_m)$ where Z is an $\ell - 1$ space in $Span(\{e_1, e_2, \ldots, e_{m-1}\})$ and $y \in Span(\{e_1, e_2, \ldots, e_{m-1}\})$. If $y \in U$ then, this contradicts the fact that $W \notin Z_m$. Then W is in the line containing $Span(Z \cup y)$ and $Span(Z \cup e_m)$. Since $Span(Z \cup y)$ and $Span(Z \cup e_m)$ are contained in $Z_{m-1} \cup Z_m$ any $W \in \mathcal{G}_{\ell,m}$ is in the 2-closure of S. □

We obtain the following corollary.

Corollary 6.2.22 *The dimension of $\mathcal{C}(\ell, m)$ is optimal among all Tanner codes on Γ_4 with an MDS $[q+1, 2, q]$ code.*

Bibliography

[ABN+92] Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ron M. Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38(2):509–516, 1992.

[Alo86] Noga Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986.

[BGH12] Peter Beelen, Sudhir R. Ghorpade, and Tom Høholdt. Duals of affine Grassmann codes and their relatives. *IEEE Transactions on Information Theory*, 58(6):3843–3855, 2012.

[BHPJ13] Peter Beelen, Tom Høholdt, Fernando Pinero, and Jørn Justesen. On the dimension of graph codes with reed-solomon component codes. In *ISIT*, pages 1227–1231, 2013.

[BZ05] Alexander Barg and Gilles Zémor. Concatenated codes: serial and parallel. *IEEE Transactions on Information Theory*, 51(5):1625–1634, 2005.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties and Algorithms*. Springer, 2007.

[DBL84] *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*. IEEE Computer Society, 1984.

[FL98] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using gröbner bases. *CODES CRYPTOGR*, 13, 1998.

[Gal63] R.G. Gallager. *Low Density Parity Check Codes*. MIT Press, 1963.

[Gei08] Olav Geil. Evaluation codes from an affine variety code perspective. In *Advances in Algebraic Geometry Codes*. World Scientific, 2008.

[GH00] Olav Geil and Tom Høholdt. Footprints or generalized Bezout's theorem. *IEEE Transactions on Information Theory*, 46(2):635–641, 2000.

[GI01] Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 658–667, 2001.

[GI02] Venkatesan Guruswami and Piotr Indyk. Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets. In *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*, pages 812–821, 2002.

[GK13] Sudhir R. Ghorpade and Krishna V. Kaipa. Automorphism groups of Grassmann codes. *Finite Fields and Their Applications*, 23(0):80 – 102, 2013.

[Gra07] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2013-11-22.

[HBG10] Tom Høholdt, Peter Beelen, and Sudhir Ramakant Ghorpade. Affine Grassmann codes. *IEEE Transactions on Information Theory*, 56(7):3166–3176, 2010.

[HJ11] Tom Høholdt and Jorn Justesen. Minimum distance of graph codes. *Springer LCNS*, 6639:201–212, 2011.

[HPZ14] Tom Høholdt, Fernando Piñero, and Peng Zeng. Optimal codes as tanner codes with cyclic component codes. *Designs, Codes and Cryptography*, pages 1–11, 2014.

[KLF01] Yu Kou, Shu Lin, and Marc P. C. Fossorier. Low-density parity-check codes based on finite geometries: A rediscovery and new results. *IEEE Transactions on Information Theory*, 47(7):2711–2736, 2001.

[Lin91] Jacobus Hendricus van Lint. *Introduction to Coding Theory*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1991.

[LRC08] Gianluigi Liva, W.E. Ryan, and M. Chiani. Quasi-cyclic generalized ldpc codes with low error floors. *Communications, IEEE Transactions on*, 56(1):49–57, January 2008.

[LU95] Felix Lazebnik and Vasiliy A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Applied Mathematics*, 60(1-3):275–284, 1995.

[Luc78] Edouard Lucas. Théorie des fonctions numériques simplement périodiques". *American Journal of Mathematics*, 1, 1878.

[Mar88] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60, 1988.

[Mat08] Sandro Mattarei. Linear recurrence relations for binomial coefficients modulo a prime. *J. Number Theor.*, 128(1):49 – 58, 2008.

[Mor94] Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular ramanujan graphs for every prime power q. *J. Comb. Theory, Ser. B*, 62(1):44–62, 1994.

[MS77] F.J. MacWillliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North Holland, 1977.

[Nil91] Alon Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207–210, 1991.

[Nog93] Dimitri Y Nogin. Codes associated to Grassmannians. *Proceedings of the International Conference held at Centre International de Rencontres de Mathématiques (CIRM), Luminy, France, June 28 - July 2, 1993*, 1993.

[Pan10] Mark Pankov. *Grassmannians of Classical Buildings*. World Scientific, 2010.

[Rot06] Ron M. Roth. *Introduction to Coding Theory*. Cambridge University Press, 2006.

[RS06] R.M. Roth and V. Skachek. Improved nearly-MDS expander codes. *Information Theory, IEEE Transactions on*, 52(8):3650–3661, Aug 2006.

[RSU01] Thomas J. Richardson, Mohammad Amin Shokrollahi, and Rüdiger L. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Transactions on Information Theory*, 47(2):619–637, 2001.

[RU01a] Thomas J. Richardson and Rüdiger L. Urbanke. The capacity of low-density parity-check codes under message-passing decoding. *IEEE Transactions on Information Theory*, 47(2):599–618, 2001.

[RU01b] Thomas J. Richardson and Rüdiger L. Urbanke. Efficient encoding of low-density parity-check codes. *IEEE Transactions on Information Theory*, 47(2):638–656, 2001.

[Rya87a] C.T. Ryan. An application of Grassmannian varieties to coding theory. *Congr. Numerantium*, 57:257–271, 1987.

[Rya87b] C.T. Ryan. Projective codes based on Grassmannian varieties. *Congr. Numerantium*, 57:273–279, 1987.

[Sei74] A. Seidenberg. Constructions in algebra. *transactions of the American Mathematical Society*, 197:273–313, 174.

[SR03] V. Skachek and R.M. Roth. Generalized minimum distance iterative decoding of expander codes. In *Information Theory Workshop, 2003. Proceedings. 2003 IEEE*, pages 245–248, March 2003.

[SS96] M. Sipser and D.A. Spielman. Expander codes. *IEEE Trans. Inf. Theory*, 42(6):1710 –1722, nov 1996.

[Sti90] Henning Stichtenoth. On the dimension of subfield subcodes. *IEEE Trans. Inf. Theory*, 36(1):90–93, 1990.

[Tan81] R. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, 27(5):533 – 547, sep 1981.

[Tan84] M. Tanner. Explicit concentrators from generalized n-gons. *SIAM J. Alg. Disc. Meth.*, 5, 1984.

[Zem01] G. Zemor. On expander codes. *IEEE Trans. Inf. Theory*, 47(2):835 –837, feb 2001.